**Oracle® Fusion Middleware**

Administrator's Guide for Oracle Adaptive Access Manager

11*g* Release 1 (11.1.1)

**E14568-08**

August 2014

ORACLE®

Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager, 11*g* Release 1 (11.1.1)

E14568-08

# Contents

## Part II  Customer Service and Forensics

## 4  Managing and Supporting CSR Cases

## 5  Investigation Using Agent Cases

# 6 Viewing Additional Details for Investigation

# Part III   Managing KBA and OTP

# 7 Managing Knowledge-Based Authentication

# 8 Enabling Challenge Questions

# 9 Setting Up OTP Anywhere

# Part IV  Managing Policy Configuration

# 10  Managing Policies, Rules, and Conditions

## 11   OAAM Security and Autolearning Policies

## 12   Managing Groups

# 13 Managing the Policy Set

# 14 Using the Scoring Engine

# 15 Creating Checkpoints

# 16 Managing System Snapshots

## Part V   Autolearning

# 17 Managing Autolearning

## 18 Managing Configurable Actions

## 19 Predictive Analysis

## Part VI   Managing Transactions

## 20   Creating and Managing Entities

## 21   Managing Transactions

## Part VII   OAAM Offline Environment

## 22   OAAM Offline

## Part VIII   Scheduling Jobs

## 23   Scheduling and Processing Jobs in OAAM

## Part IX   Reporting

## 24   Using the Dashboard

## 25   Configuring BI Publisher Reports

# 26 Monitoring Performance by Using Fusion Middleware Control

# 27 Monitor and Audit of Events

# Part X   Deployment Management

# 28 Using the Properties Editor

# Part XI   Command-Line Interface

# 29 Oracle Adaptive Access Manager Command-Line Interface Scripts

# Part XII   Multitenancy

# 30 Multitenancy Access Control for CSR and Agent Operation

# Part XIII   Troubleshooting

# 31 FAQ/Troubleshooting

# Part XIV   Appendixes

# A   Access Roles

# B   Pattern Processing

# C   Conditions Reference

# D  Oracle Adaptive Access Manager Reports Reference

# E  The Discovery and OAAM Policy Development Processes

# F  Globalization Support

# G  Oracle Adaptive Access Manager Properties

# H  Device Fingerprinting

# I  Setting Up Archive and Purge Procedures

# J  Configuring SOAP Web Services Access

# K  Configuring Logging

# L  Rule and Fingerprint Logging

# Index

# Preface

The *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager* provides in-depth information on administering and using Oracle Adaptive Access Manager's set of tools for fraud monitoring and detection.

## Audience

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

| Users | Description |
|---|---|
| Investigators and Support Personnel | Investigators (Fraud Investigators and Fraud Investigation Managers) and support personnel (CSR and CSR Managers) use Oracle Adaptive Access Manager's case management tools to handle security and customer cases day-to-day. They have detailed knowledge about user activity and security issues. Security Administrators work with Investigators and support personnel to identify if policies need to be adjusted or new policies need to be created. |
| Security Administrators | Security Administrators (Rule Administrators) gather intelligence from various sources to identify needs and develop requirements to address them. Some sources for intelligence include Investigators, industry reports, antifraud networks, compliance mandates, and company polices.

Security Administrators plan, configure and deploy policies based on the requirements from analysts. |
| System Administrator | System Administrators configure environment-level properties and transactions. |

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

### Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

## Related Documents

For more information, see the following documents in the Oracle Fusion Middleware 11g Release 1 (11.1.1) documentation set:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*

- *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*

- *Oracle Fusion Middleware Administrator's Guide*

- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*

- *Oracle Fusion Middleware High Availability Guide*

- *Oracle Fusion Middleware Upgrade Planning Guide*

- *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*

- *Oracle Fusion Middleware Reference for Oracle Identity Management*

## Conventions

The following text conventions are used in this document:

| Convention | Meaning |
| --- | --- |
| **boldface** | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. |
| *italic* | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| `monospace` | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

# What's New in Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1)?

This chapter introduces the new and changed administrative features of Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1). It contains these topics:

- New Features for Oracle Adaptive Access Manager 11g Release 1 (11.1.1)
- Feature Comparison Chart - Oracle Adaptive Access Manager 11g vs. Oracle Adaptive Access Manager 10g
- Concepts and Terminology Changes for Oracle Adaptive Access Manager 11g

## New Features for Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1)

Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1) includes many important features and enhancements that were not available with Oracle Adaptive Access Manager 10*g*. The following is a list of the new features and enhancements:

| Areas | Features and Enhancements |
|-------|---------------------------|
| Interface | The new rich Oracle Adaptive Access Manager user interface provides<br>■ Navigation and Policy trees, which allow quick and visible access to features<br>■ Tabs and accordion panels that reduce real estate usage for multitasking<br>■ Streamlined flows that capture use case flows of execution. For example, the flow for rules is search, create, edit, and copy rules<br>■ Improved search and filtering, where you can save searches and filter directly on columns<br>■ New and improved screens in Oracle Adaptive Access Manager. Oracle Adaptive Access Manager provides enhanced usability for fraud analysis and forensic operations<br>■ Advanced table display controls to add and remove columns, reposition and resize columns, and detach columns<br>■ Additional search filters for alert messages, geographic location, and IP range<br>■ Export feature that enables search results to be exported to an Excel file format<br>■ New "Add to Group" feature in search sessions and details pages that enables entities to be added to groups easily<br>■ Direct access to documentation from Oracle Adaptive Access Manager |

| Areas | Features and Enhancements |
|---|---|
| Security Policies | Newly updated security policies that incorporate:<br><br>■ Patterns and other techniques to improve the accuracy and risk analysis<br><br>■ Oracle Data Miner along with new rule conditions and improved learning patterns to create a unique and optimized real-time risk analytics solution more capable of profiling behaviors than previous versions |
| Policy Creation | New features in policy creation enables you to:<br><br>■ Copy policies to checkpoints<br><br>Policies can be copied to other checkpoints. When policies are copied, all the details are copied including the nested policies, trigger combinations, preconditions, group linking, and others<br><br>■ Configure trigger combinations more easily<br><br>The new design enables you to more easily define and manage trigger combinations and allows the appending or overriding of actions and alerts<br><br>■ Execute nested conditions<br><br>New conditions support the execution of nested policies<br><br>■ View indicators<br><br>Indicators are available to show the number of policies linked to a policy, rules, trigger combinations, group linking, conditions in policies, and so on |
| Rule Creation | Rules are now much easier to create.<br><br>■ Rule creation has been simplified with the removal of rule templates from the product.<br><br>■ Rules can be copied to different policies under any checkpoint |
| OTP Anywhere | OTP Anywhere can create universal delivery options for auto-generated one-time-passwords used for secondary, risk-based user challenges to add sophisticated security to basic authentication flows. |
| Investigation | New investigation tools have been added to make investigations quicker and easier<br><br>■ Details screen that allow investigators, security administrators, and other power users to cross reference on data points to find related data in a quick and easy way<br><br>■ The new agent cases that make forensic investigations quicker, easier and more successful. Events can be configured to create a case automatically. An investigator can quickly view the data involved in an incident and quickly locate related situations by easily harnessing the complex data relationships captured by OAAM |
| Encryption Keys | Encryption keys required by Oracle Adaptive Access Manager can be securely managed using Fusion Middleware Control without having to create Keystore files |
| Universal Risk Snapshot | Snapshots can be created allowing security administrators to simply and easily migrate security data across environments or restore security configuration to a known state |
| Multitenancy | Multitenant access controls for customer service representative interface to allow protection of multiple application tenants with a single instance of OAAM |
| OAAM Batch Risk Analysis | Oracle Adaptive Access Manager batch risk analysis tool to be used as:<br><br>■ A standalone security tool to analyze, detect and alert high risk transactions<br><br>■ A research and development tool to create and verify new policies and rules using offline customer data without impacting customers in real-time environment<br><br>■ A supplemental batch analysis tool in the tuning of rules and verification of rules behavior against real customer and transaction data without impacting customers in real-time environment |

| Areas | Features and Enhancements |
|---|---|
| Audit | Most of the administrative operations are now audited using Oracle Audit Service. Audit events can be viewed using the standard audit reports. |
| Web Services | Oracle Adaptive Access Manager Web services are implemented using Oracle Web Services. |
| Application Logging | Oracle Adaptive Access Manager 11g uses Java logging instead of log4j. Logging can be configured using Fusion Middleware Control. |
| Integration with the Dynamic Monitoring System | Some performance metrics are now integrated with Dynamic Monitoring System. These metrics and related reports can be viewed using Fusion Middleware Control |

# Feature Comparison Chart - Oracle Adaptive Access Manager 11*g* vs. Oracle Adaptive Access Manager 10*g*

| Features | 10.1.4.3 | 10.1.4.5 | 11g (11.1.1) |
|---|---|---|---|
| Real-time and offline rules engine | X | X | X |
| Virtual authentication devices | X | X | X |
| Knowledge-based authentication | X | X | X |
| Adaptive device identification* | X | X | X |
| Base security policies (ongoing updates) | X | X | X |
| Real-time dashboard (improved) | X | X | X |
| Customer service module | X | X | X |
| Real-time access to activity data | X | X | X |
| Actions, alerts, and risk scoring | X | X | X |
| Rule conditions | | X | X |
| Optimized log data management | | X | X |
| Enhanced caching of rules data object | | X | X |
| Expanded integration APIs | | X | X |
| Investigation agent workflow | | X | |
| Rules authoring user interface | | X | X |
| Transaction definition and mapping user interface | | X | X |
| Data entity definition and mapping user interface | | X | X |
| Behavior pattern configuration interface | | X | X |
| Configurable actions | | X | X |
| Server-generated one-time password | | X (Native only) | X (All deployment types) |
| Customizable reporting BI Publisher (bundled) | | X | X |
| Tree-based navigation and policy browse | | | X |
| Tabular multitasking user interface | | | X |
| Customizable search screens | | | X |

| Features | 10.1.4.3 | 10.1.4.5 | 11g (11.1.1) |
|---|---|---|---|
| Common audit framework | | | X |
| Oracle Installer and Repository Creation Utility | | | X |
| Oracle Patch | | | X |
| Oracle Adaptive Access Manager Offline User Interface | X | X | X |
| Document Models | X | X | |
| Globalization | | X | X |

| Integrations | 10.1.4.3 | 10.1.4.5 | 11g (11.1.1) |
|---|---|---|---|
| Oracle Access Manager integration | X | X | X |
| Oracle Identity Manager integration | | | X |

# Concepts and Terminology Changes for Oracle Adaptive Access Manager 11*g*

Customers migrating from Oracle Adaptive Access Manager 10*g* to 11*g* will notice a few key conceptual and terminology changes. These changes are intended to align terminology used across the Identity Management suite products and simplify administration. Full definitions of these and many other terms can be found in the glossary.

### General Term Changes

| 10*g* Term | 11*g* Term |
|---|---|
| runtime | checkpoint |
| | A checkpoint is a specified point in a session when Adaptive Access Manager collects and evaluates security data using the rules engine. |
| model | policy |
| | Policies contain security rules and configurations used to evaluate the level of risk at each checkpoint. |
| manual override | trigger combination |
| | Trigger combinations are additional results and policy evaluation that are generated if a specific sequence of rules trigger. |
| Application ID | Organization ID |
| | From the administration perspective, each application/primary user group is translated into an "Organization ID." The term, "Application ID" has been renamed as "Organization ID," which represents the primary user group of a particular user. |
| | For the OAAM Server side, the term "Application ID" remains the same as before. When communicating with proxies, OAAM Server passes the Applications ID, which uniquely identifies an application. |

### Concept Changes

Concepts changes are listed in the following table.

| 10*g* Concept | 11*g* Concept |
|---|---|
| OAAM Adaptive Risk Manager | The rules engine is now part of OAAM Server. The Administration Console is now a separate application named OAAM Admin. |
| OAAM Adaptive Strong Authenticator | The end-user flows including the virtual authentication devices, Knowledge-Based Authentication and One-Time Password authentication are now contained in OAAM Server. |
| rule template | The concept has been removed from product |
| policy type | The concept has been removed from the product |

### Web Applications

Oracle Adaptive Access Manager's deployed applications in 11*g* are:

- OAAM Server - Adaptive Risk Manager, Adaptive Strong Authenticator, Web services, LDAP integration and user Web application used in all deployment types except native integration

- OAAM Admin - Administration Web application for all environment, Adaptive Strong Authenticator and Adaptive Risk Manager features

### Architecture and Deployment Changes

Architecture and deployment changes are listed as follows:

- Administration User Interface is now a separate Web application called *OAAM Admin*.

- Adaptive Strong Authenticator is now deployed as part of the *OAAM Server* Web application.

- OAAM Web applications are now packaged as `.ear` files. Exploding them is neither recommended nor supported.

# Part I

# Getting Started with Oracle Adaptive Access Manager

This part of the book provides an introduction to the Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1).

Part I contains the following chapters:

- Chapter 1, "Introduction to Oracle Adaptive Access Manager"
- Chapter 2, "Setting Up the Oracle Adaptive Access Manager Environment for the First Time"
- Chapter 3, "Oracle Adaptive Access Manager Navigation"

# 1

# Introduction to Oracle Adaptive Access Manager

Oracle Adaptive Access Manager protects companies exposing Web applications and services, and their end users from online threats and insider fraud. It provides risk-aware authentication, real-time behavior profiling, and transaction and event risk analysis.

Functionality can be divided into two major areas as summarized in Table 1–1.

**Table 1–1    Oracle Adaptive Access Manager Functionality**

| Functionality | Description |
| --- | --- |
| Real-time or offline risk analysis | Oracle Adaptive Access Manager provides functionality to calculate the risk of an access request, an event or a transaction, and determine proper outcomes to prevent fraud and misuse. A portion of the risk evaluation is devoted to verifying a user's identity and determining if the activity is suspicious. |
| | Functionality that support risk analysis are: |
| | ■ Rules Engine |
| | ■ Entities |
| | ■ Transactions |
| | ■ Patterns |
| | ■ Alerts |
| | ■ Actions |
| | ■ Configurable actions |
| End-user facing functionality to prevent fraud | Oracle Adaptive Access Manager protects end users from phishing, pharming, and malware. The virtual authentication devices secure credential data at the entry point; this ensures maximum protection because the credential never resides on a user's computer or anywhere on the Internet where it can be vulnerable to theft. As well, Oracle Adaptive Access Manager provides interdiction methods including risk-based authentication, blocking and configurable actions to interdict in other systems. |
| | Functionality that supports end-user facing security are: |
| | ■ Virtual authentication devices |
| | ■ Knowledge-Based Authentication (KBA) |
| | ■ OTP Anywhere |
| | ■ Security policies |

This chapter provides an overview of Oracle Adaptive Access Manager 11*g* and includes the following topics:

- Benefits of Oracle Adaptive Access Manager
- Oracle Adaptive Access Manager Features
- Oracle Adaptive Access Manager Architecture
- Deployment Options

## 1.1 Benefits of Oracle Adaptive Access Manager

Oracle Adaptive Access Manager is a security solution to protect the enterprise and its end users of the Web applications and services it exposes.

Oracle Adaptive Access Manager provides:

- Risk-aware authentication
- Authentication security
- Real-time and offline risk analytics
- Flexible deployment options
- Out-of-the-box integrations with single sign-on and identity management

The following illustration shows the functionalities contained in OAAM Server and OAAM Admin.

*Figure 1–1   Security Solution*

## 1.2 Oracle Adaptive Access Manager Features

Adaptive access systems can provide the highest levels of security with context-sensitive online authentication and authorization. Thus, situations are evaluated and proactively acted upon based on various types of data.

This section outlines key components/features used for authentication and fraud monitoring and detection.

### Application Access Security

Oracle Adaptive Access Manager provides a number of rich features that strengthen existing web application login flows. Regardless of the type of authentication in place, Oracle Adaptive Access Manager can improve the level of security in a usable manner. Insider fraud, session hijacking, stolen credentials and other threats cannot be eliminated by strong, credential based authentication alone. Adding a risk-based challenge layer behind existing authentication can increase the level of security with minimal impact to the user experience – a critical factor for large deployments where desk calls can impact the bottom line. Oracle Adaptive Access Manager's suite of virtual authentication devices combats phishing personalized images and phrases known only to the server and the end user. Furthermore, through the use of KeyPad and PinPad, security of the user's credentials during entry can be assured by not capturing or transmitting the actual credential of the end user. This protects the credential from theft by malware and other similar threats. The virtual authentication devices are server driven; all features are provided without any client-side software or logic that can be compromised by key-loggers and other common malware. Additionally, Oracle Adaptive Access Manager performs device fingerprinting and behavioral profiling on every access to determine the likelihood that the authentication is being attempted by the valid user.

### Device Fingerprinting

Oracle Adaptive Access Manager contains proprietary clientless technologies for fingerprinting and interrogating devices used during access requests and transactions. Device fingerprinting is a mechanism to recognize the devices a customer uses whether it is a desktop computer, laptop computer or other web-enabled device.

Each time the user accesses the system, information about the device is collected. OAAM generates a unique single-use fingerprint and marks a device for each user session. It is replaced upon each subsequent fingerprinting process with another unique fingerprint.

The fingerprinting process can be run any number of times during a user session to allow detection of changes mid-session that can indicate session hijacking. OAAM monitors a comprehensive list of device attributes. If any attributes are not available the device can still be fingerprinted. The single-use capabilities combined with server-side logic defends against the fingerprint being stolen and reused on another machine to commit fraud.

### Answer Logic

Answer Logic increases the usability of Knowledge Based Authentication (KBA) questions by accepting answers that are fundamentally correct but may contain a small typo, abbreviation or misspelling. For example, if abbreviation is enabled in Answer Logic a user is challenged with the question "What street did you live on in high school?" They may answer "1st St." which is fundamentally correct even though when they registered the answer six months ago they entered "First Street". By allowing a configurable variation in the form of correct answers, Answer Logic

dramatically increases the usability of registered challenge questions making the balance between security and usability firmly in the control of the enterprise.

### OTP Anywhere

OTP Anywhere allows end users to authenticate themselves by entering a server generated one-time-password (OTP) which they can receive via SMS, email, instant message or voice channels. When the OTP is sent via SMS, the user's cell phone serves as a physical second factor that the user has in their possession. As well, the authentication is being sent out-of-band to increase the level of assurance that only the valid user has access to the one-time password. When authentication methods such as Answer Logic and OTP Anywhere are applied based on the level of risk it can dramatically increase web application access security in a cost-effective and usable manner.

### Dashboard

The Oracle Adaptive Access Manager Dashboard is a unified display of integrated information from multiple components in a user interface that organizes and presents data in a way that is easy to read. The Oracle Adaptive Access Manager dashboard present monitor data versions of key metrics. Administrators can easily see up-to-the-minute data on application activity from a security perspective. The reports that are presented help users visualize and track general trends.

### Case Management

Oracle Adaptive Access Manager provides a framework and set of tools for investigators and customer service representatives.

The Case Management feature of Oracle Adaptive Access Manager is used in two ways.

- Users of the enterprise using Oracle Adaptive Access Manager can call the enterprise asking for assistance with customer-facing features of Oracle Adaptive Access Manager such as images, phrases, or challenge questions, or any issues with their account. The CSR uses Case Management to create a case which records all the actions performed by the CSR to assist the user as well as various account activities of the user.

- The Case Management feature is also used by Fraud Investigators to investigate potentially fraudulent activity performed on user accounts.

### Knowledge-Based Authentication

Oracle Adaptive Access Manager provides out-of-the-box secondary authentication in the form of knowledge-based authentication (KBA) questions. The KBA infrastructure handles registration, answers, and the challenge of questions. Since KBA is a secondary authentication method, it is presented after successful primary authentication.

KBA is used to authenticate an individual based on knowledge of personal information, substantiated by a real-time interactive question and answer process. Oracle Adaptive Access Manager's Rules Engine and organizational policies are responsible for determining if it is appropriate to use challenge questions to authenticate the customer.

### Policy Management

Policies and rules can be used by organizations to monitor and manage fraud or to evaluate business elements. The policy and rules are designed to handle patterns or practices, or specific activities that you may run across in the day-to-day operation of

your business. Using Oracle Adaptive Access Manager, you can define when the collection of rules is to be executed, the criteria used to detect various scenarios, the group to evaluate, and the appropriate actions to take when the activity is detected.

### Predictive Analysis

Oracle Adaptive Access Manager integrates with Oracle Data Mining to provide statistical risk analysis in real-time. This form of risk analysis "trains" over time so it compliments the highly configurable rules and behavioral profiling which do not require training. The more training each model does, the more accurate the risk analysis becomes. The out of the box predictive models are trained in two ways:

- The anomaly detection model trains automatically when fed historical access data.

- The fraud classification model trains on the findings of human fraud investigators. Additional models can be configured as required to meet specific deployment use cases. This open approach to predictive risk analysis allows OAAM customers to clearly see on which decisions outcomes are based and allows augmentation as required.

This open approach to predictive risk analysis allows OAAM customers to clearly see on which decisions outcomes are based and allows augmentation as required.

### Configurable Actions

Configurable actions are actions that are triggered based on the result action or risk scoring or both after a checkpoint execution. Java classes and action templates for certain configurable actions are provided out-of-the-box, but you have the option to create configurable actions based on business requirements.

### Transaction Definition

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 types of details are involved. Before the client-specific transaction with its corresponding entities can be captured and used for enforcing authorization rules, fraud analysis, and so on, it must be defined and mapped. Oracle Adaptive Access Manager's Transactions feature allows administrators to perform this task. With the Transaction Definition feature, an administrator is able to create entity and data element definitions and map them to the client-specific data (source data).

### Reports

Reporting is available through Oracle Adaptive Access Manager. A limited license of Oracle Business Intelligence Publisher is included for customizable reporting capabilities.

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.

## 1.3 Oracle Adaptive Access Manager Architecture

Oracle Adaptive Access Manager is designed to provide a rich selection of capabilities with heterogeneous support for a variety of environments. Functionality is implemented to optimize resources and provide enterprise class scalability and redundancy.

### 1.3.1 High Availability

Oracle Adaptive Access Manager is built on a J2EE-based, multi-tier deployment architecture that separates the platform's presentation, business logic, and data tiers. Because of this separation of tiers, Oracle Adaptive Access Manager can rapidly scale with the performance needs of the customer. The architecture can leverage the most flexible and supported cross-platform J2EE services available: a combination of Java, XML and object technologies. This architecture makes Oracle Adaptive Access Manager a scalable, fault-tolerant solution.

The runtime components including the rules engine and end user interface flows are contained in one managed server while the administration console functionality is separated out into its own managed server. The administration console contains the customer service and security analyst case management functionality which must always be available to employees in potentially large call centers with high call volumes.

Depending on the deployment method used the topology changes slightly. Native application integration deployments embed the runtime components so the administration console is the only additional managed server added to the deployment. Oracle Adaptive Access Manager is also completely stateless and fully supports clustered deployments to meet high performance requirements. As well, all high availability features of the Oracle database are supported for use with Oracle Adaptive Access Manager.

## 1.4 Deployment Options

Oracle Adaptive Access Manager supports a number of deployment options to meet the specific needs of practically any deployment. The decision of which deployment type to employ is usually determined based on the use cases required and the applications being protected.

In the Oracle Adaptive Access Manager architecture shown in Figure 1–2, end users access customer web applications in various deployments.

*Figure 1–2   Sample deployment scenario for performance and scalability*
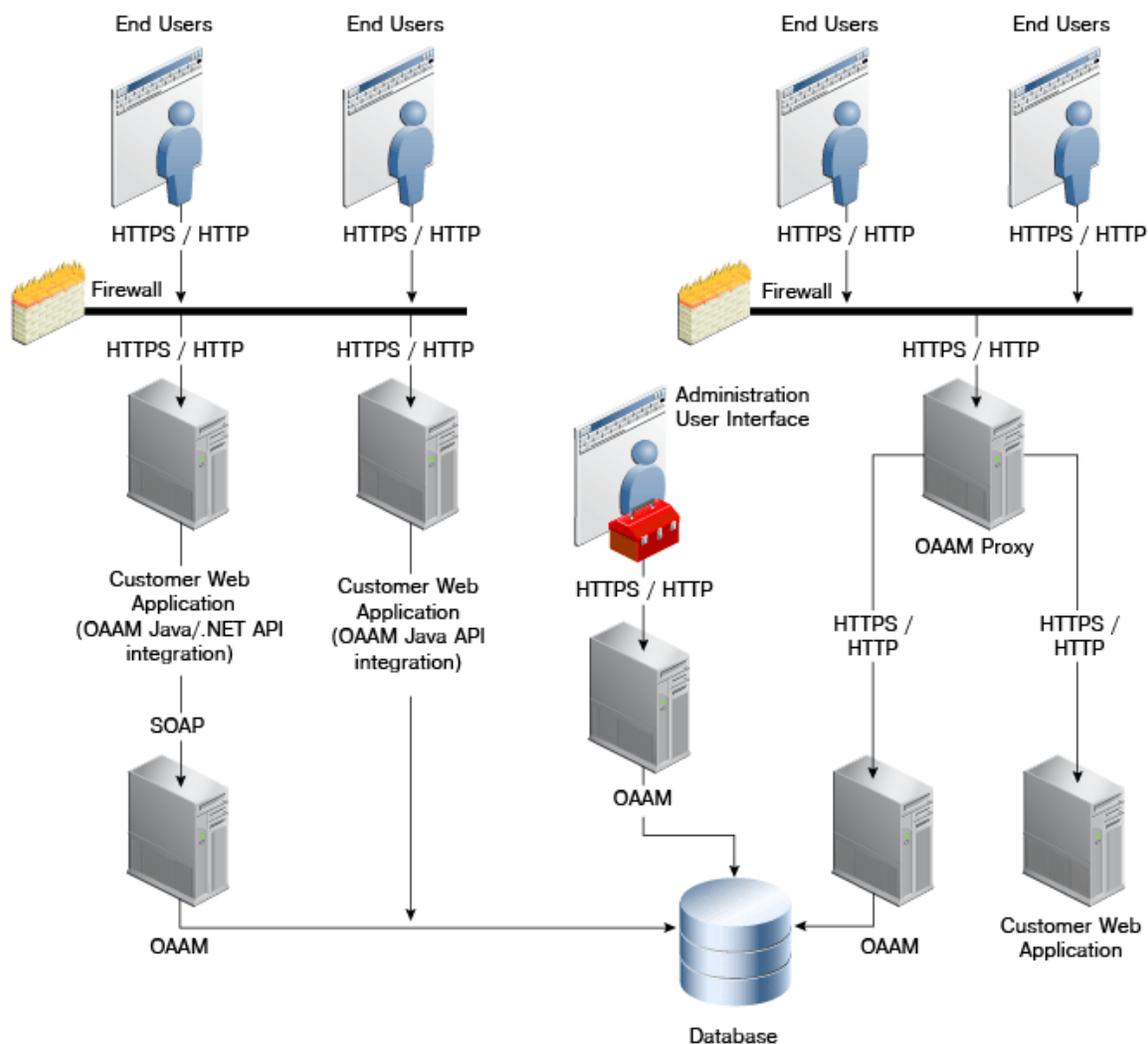


## 1.4.1  Single Sign-On Integration

Oracle Adaptive Access Manager has an out of the box integration with Oracle Access Manager to provide advanced login security including the virtual devices, device fingerprinting, real-time risk analysis and risk-based challenge. New to 11*g* there are two versions of the OAAM and OAM integration, basic and advanced. The "basic" integration embeds OAAM into the OAM runtime server. It includes many of the login security use cases available from OAAM and reduces the footprint. To gain advanced features and extensibility customers can deploy using the "advanced" integration. Features such as OTP anywhere, challenge processor framework, shared library framework and secure self-service password management flows require the advanced integration option. Oracle Adaptive Access Manager can also be integrated with third party single sign-on products via systems integrators if required.

## 1.4.2  Universal Installation Option Reverse Proxy

Oracle Adaptive Access Manager can be deployed using an Apache module to intercept login requests and provide advanced login security. The flows available are the same as for the advanced single sign-on integration option.

The main benefit of the Oracle Universal Installation Option (UIO) deployment is that it requires little or no integration with protected applications and SSO is not required.

### 1.4.3 Native Application Integration

Oracle Adaptive Access Manager can be natively integrated with an application to provide extreme high performance and highly customizable security. A native integration embeds OAAM in-process inside the protected applications. The application invokes the Oracle Adaptive Access Manager APIs directly to access risk and challenge flows.

### 1.4.4 Web Services Application Integration

Customers who have advanced requirements similar to native integration but who prefer to use SOAP web services instead of Java API integration directly can choose this option.

# 2

# Setting Up the Oracle Adaptive Access Manager Environment for the First Time

All tasks in this book presume that you have Oracle Adaptive Access Manager 11*g* installed with initial configuration completed as described in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

This chapter presents details on setting up the Oracle Adaptive Access Manager environment for first time users. For information on how to upgrade an existing Oracle Adaptive Access Manager 10*g* (10.1.4.5) to Oracle Adaptive Access Manager 11*g* Release 1, refer to the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*.

## 2.1 Installation and Configuration

The *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* 11*g* Release 1 (11.1.1) provides all installation and initial configuration details.

Oracle Adaptive Access Manager is installed into an environment where you may install other Oracle Identity Management 11*g* components.

The following Oracle Adaptive Access Manager-related components are deployed in a new WebLogic administration domain using the Oracle Fusion Middleware Configuration Wizard:

- WebLogic Administration Server
- Managed Server for Oracle Adaptive Access Manager
- Oracle Adaptive Access Manager Console deployed on the Administration Server

For information on how to install and configure Oracle Adaptive Access Manager, see the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

## 2.2 Setting Up the Oracle Adaptive Access Manager Base Environment

After installing and configuring Oracle Adaptive Access Manager, you must complete the following tasks to set up the initial base Oracle Adaptive Access Manager environment.

Procedures are provided in the following sections:

- Setting Up CLI Environment
- Setting Up Encryption and Database Credentials for Oracle Adaptive Access Manager
- Creating OAAM Users

- Importing the OAAM Snapshot

- Importing IP Location Data

- Enabling OTP

- Setting the Time Zone Used for All Time Stamps in the Administration Console

## 2.3 Setting Up CLI Environment

The Oracle Adaptive Access Manager Command-Line Interface (CLI) scripts enable users to perform various tasks instead of using the Oracle Adaptive Access Manager Administration Console.

For information on setting up the CLI environment, see Section 29.2, "Setting Up the CLI Environment."

## 2.4 Setting Up Encryption and Database Credentials for Oracle Adaptive Access Manager

Encryption is used to protect data within Oracle Adaptive Access Manager from unauthorized access. The process uses methods and a key or keys to encode plain text into a non-readable form. A key is required to decrypt the encrypted information and make it readable again. Authorized persons who possess the key can decrypt information that is encrypted with the same key.

This section provides instructions to set up encryption and database credentials for Oracle Adaptive Access Manager.

### 2.4.1 Overview of the Process

An overview for setting up encryption and database credentials is provided in this section.

#### 2.4.1.1 Setting up Encryption

Setting up encryption involves the following steps:

- Ensure the secret keys (a.k.a symmetric keys) for both the configuration value and database are available. If you do not have a secret key, generate an encoded symmetric key using the `genEncodedKey` command.

- Encode the key using the `base64encode` option of the `encodeKey` command. This step is not required if the `genEncodedKey` command was used to generate the key.

- Use the Fusion Middleware Control to add the encoded secret key to an alias in the Credential Store Framework in the domain where Oracle Adaptive Access Manager is installed.

  A credential store is a repository to store user name/password or generic credentials (a certificate). The value of using a credential store is that the application does not store passwords in clear text and does not have to invent its own solutions for protecting passwords, allowing administrators and developers alike to work with a consistent credential repository.

### 2.4.1.2 Configuring Database Credentials in the Credential Store Framework

Configuring database credentials in the Credential Store Framework involves the following steps:

- Use the Fusion Middleware Control to add database credentials (user name and password) in the Credential Store Framework in the domain where Oracle Adaptive Access Manager is installed. These credentials are used by the Oracle Adaptive Access Manager command-line utilities.

- Configure the properties files that are used by the Oracle Adaptive Access Manager CLI utilities with details of the WebLogic administration server and Oracle Adaptive Access Manager database.

For information on the credential store, refer to "Managing the Credential Store" in the *Oracle Fusion Middleware Application Security Guide*.

## 2.4.2 Prerequisites

Prerequisites for setting up encryption and database credentials for Oracle Adaptive Access Manager are:

1. If you do not have access to the Oracle Adaptive Access Manager installation folder, make sure Oracle Adaptive Access Manager 11*g* is configured with Fusion Middleware Control while creating the domain.

2. If you have access to the Oracle Adaptive Access Manager installation folder then make sure you have access to running the command-line scripts in the *MW_HOME\IDM_ORACLE_HOME*\oaam\cli folder.

3. Make sure Sun JDK is installed and check that the java command is in the path by executing the java command.

---

> **Note:** If you are upgrading from Oracle Adaptive Access Manager 10.1.4.5 to Oracle Adaptive Access Manager 11*g*, you can skip Section 2.4.3, "Setting up Secret Key for Encrypting Configuration Values,", Section 2.4.4, "Setting Up Secret Key for Encrypting Database Values,"and Section 2.4.5, "Generating an Encoded Secret Key," since the Upgrade Assistant automatically migrates the secret keys from Oracle Adaptive Access Manager 10.1.4.5 to the Credential Store Framework in Oracle Adaptive Access Manager 11*g*.

---

## 2.4.3 Setting up Secret Key for Encrypting Configuration Values

To set up the secret key for encrypting configuration values, follow the steps in this section:

1. Go to the Oracle Adaptive Access Manager command-line folder *MW_HOME\IDM_ORACLE_HOME*\oaam\cli.

2. Create a file config_secret_key.file and add the secret key to the file by entering:

   tobase64=<secret-key>

> **Note:** ■ If you do not have any secret key refer to Section 2.4.5, "Generating an Encoded Secret Key."
>
> ■ This is your key to the encryption algorithm.
>
> ■ Note that 3DES accepts any key, but it must be a minimum of 24 characters.

3.  Encode the key using the Base64 algorithm by executing the following command.

    **a.** In Unix

    ```
    encodeKey.sh config_secret_key.file
    ```

    **b.** In Windows

    ```
    encodeKey.cmd config_secret_key.file
    ```

    If the encoding command was successful, you see output similar to the following:

    ```
    base64encode is done!
    Base64 Encoded value =<encoded_value>
    ```

    If the `KeyStore` command was not successful, you might see the following error:

    ```
    Exception in thread "main" java.lang.NoClassDefFoundError: while resolving
    class: com.bharosa.vcrypt.common.util.KeyStoreUtil at
    java.lang.VMClassLoader.resolveClass(java.lang.Class)
    (/usr/lib/libgcj.so.5.0.0) at java.lang.Class.initializeClass()
    (/usr/lib/libgcj.so.5.0.0) at java.lang.Class.forName(java.lang.String,
    boolean, java.lang.ClassLoader) (/usr/lib/libgcj.so.5.0.0) at
    java.lang.Class.forName(java.lang.String) (/usr/lib/libgcj.so.5.0.0)
    ```

4.  Note down the encoded value of the key printed on the screen. Make sure there are no spaces. You need this to add to the Credential Store Framework.

5.  Refer to Section 2.4.6, "Adding Symmetric Key to the Credential Store Framework" for instructions to add the encoded key to the Credential Store Framework.

## 2.4.4 Setting Up Secret Key for Encrypting Database Values

To set up the secret key for encrypting database values:

1.  Go to the Oracle Adaptive Access Manager command-line folder *MW_HOME\IDM_ORACLE_HOME*\oaam\cli.

2.  Create a `file db_secret_key.file` and add the secret key to the file by entering:

    tobase64=<secret-key>

> **Note:** ■ If you do not have any secret key refer to Section 2.4.5, "Generating an Encoded Secret Key."
>
> ■ This is your key to the encryption algorithm.
>
> ■ Note that 3DES accepts any key, but it must be a minimum of 24 characters.

3. Encode the key using Base64 algorithm by executing the following command.

   a. In Unix

   ```
   encodeKey.sh db_secret_key.file
   ```

   b. In Windows

   ```
   encodeKey.cmd db_secret_key.file
   ```

   If the encoding command was successful, you see output similar to the following:

   ```
   base64encode is done!
   Base64 Encoded value = <encoded_value>
   ```

   If the `KeyStore` command was not successful, you might see the following error:

   ```
   Exception in thread "main" java.lang.NoClassDefFoundError: while resolving
   class: com.bharosa.vcrypt.common.util.KeyStoreUtil at
   java.lang.VMClassLoader.resolveClass(java.lang.Class)
   (/usr/lib/libgcj.so.5.0.0) at java.lang.Class.initializeClass()
   (/usr/lib/libgcj.so.5.0.0) at java.lang.Class.forName(java.lang.String,
   boolean, java.lang.ClassLoader) (/usr/lib/libgcj.so.5.0.0) at
   java.lang.Class.forName(java.lang.String) (/usr/lib/libgcj.so.5.0.0)
   ```

4. Note down the encoded value of the key printed on the screen. Make sure there are no spaces. You need this to add to the Credential Store Framework.

5. Refer to Section 2.4.6, "Adding Symmetric Key to the Credential Store Framework" for instructions on adding the encoded key to the Credential Store Framework.

### 2.4.5 Generating an Encoded Secret Key

To generate an encoded secret key:

1. Execute the following command:

   a. In Unix

   ```
   genEncodedKey.sh sample.db_3des_input.properties
   ```

   b. In Windows

   ```
   genEncodedKey.cmd sample.db_3des_input.properties
   ```

2. If the command is successful you see output similar to the following:

   ```
   Generated key = <encoded_key>
   ```

   ---

   **Note:** Encoding the generated key is not necessary since it is already encoded.

   ---

### 2.4.6 Adding Symmetric Key to the Credential Store Framework

OAAM Servers automatically generate the secret key if you start them after domain creation. You can choose to use those autogenerated secret keys if you do not want to use different secret keys.

To add symmetric key to the Credential Store Framework:

1. Log in to Fusion Middleware Control at http://*weblogic_admin_server*:*port*/em using the Web browser and use the WebLogic Administrator credentials to log in.

2. Expand the **WebLogic Domain** icon in the Navigation tree in the left pane.

3. Select **OAAM domain** and right-click and select the menu option **Security**, and then the option **Credentials** in the submenu.

4. Check if there is a map with the name **oaam**. If not, click the **Create Map** option and enter the Map Name as oaam. Click **OK** to save the map.

5. Click **oaam** to select the map and then click **Create Key**.

6. In the pop-up dialog make sure **Select Map** is **oaam**.

7. Enter:

   ■ **Key Name**: DESede_db_key_alias if the key is database-related or DESede_config_key_alias if it is configuration/application related. Make sure there are no typos or spaces.

   ■ **Type**: Generic.

   ■ **Credential Value**: encoded value of the symmetric key

8. Enter a description in the **Description** field.

9. Click **OK** to save the secret key to the Credential Store Framework.

10. Make sure you back up the alias and the secret key.

   The backup is required if you must recreate the domain and point the domain to the existing Oracle Adaptive Access Manager database.

   > **Note:** If you lose the secret key, all the existing data in the Oracle Adaptive Access Manager database becomes unusable since many important administrative operations involve encrypted data.

## 2.4.7 Setting Up Oracle Adaptive Access Manager Database Credentials in the Credential Store Framework

To set up the Oracle Adaptive Access Manager database credentials in the Credential Store Framework:

1. Log in to Fusion Middleware Control at http://*weblogic_admin_server*:*port*/em using the Web browser and use the WebLogic Administrator credentials to log in.

2. Expand the **WebLogic Domain** icon in the Navigation tree in the left pane.

3. Select the **OAAM domain** and right-click and select the menu option **Security** and then the option **Credentials** in the submenu.

4. Check to see whether there is a map with the name **oaam**. If not click the **Create Map** option and enter the **Map Name** as oaam. Click **OK** to save the map.

5. Click **oaam** to select the map and then click **Create Key**.

   OAAM Servers automatically generate the secret key if you start them after domain creation. You can choose to use those auto-generated secret keys if you do not want to use different secret keys.

6. In the pop-up dialog make sure **Select Map** is **oaam**.

7. Enter the following:

   ■ **Key**: oaam_db_key. Make sure there are no typos and spaces.

   ■ **Type**: Password

- **UserName**: database user name of OAAM

- **Password**: database password of OAAM

8. Enter the description.

9. Click **OK** to save the secret key to the Credential Store Framework.

### 2.4.8 Backing Up Secret Keys and Database and Configuration Keys

You must back up the secret keys used. You may need these keys, if you have to recreate the Oracle Adaptive Access Manager 11g domain. Make sure you note the secret key and the alias name.

1. Log in to Oracle Enterprise Manager.

2. Expand the WebLogic Domain on the left pane, and select **OAAM** domain.

3. From the OAAM Domain, select **Security**, and then **Credentials**.

4. Expand **oaam** and select the symmetric key related entries associated with the Type **Generic**.

5. Click **Edit**.

6. Go to the **Credentials** section then copy the symmetric key related entries and note the key name.

7. Repeat the above steps to back-up database and configuration keys.

> **Note:** If you delete and recreate the Oracle Adaptive Access Manager 11g domain, make sure you use the backed-up secret keys when setting the encryption keys so that the existing data in the Oracle Adaptive Access Manager database can be decrypted properly.

## 2.5 Creating OAAM Users

Before you can access the Oracle Adaptive Access Manager Administration Console, you must create users. Creating these users allows you to use OAAM.

The user can be created in the WebLogic Administration Console. Details for creating an administration user in the WebLogic Administration Console are provided below.

If you want to take care of user and group creation in the external LDAP store, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

You create a user as follows:

1. Log in to the Oracle WebLogic Administration Console for your WebLogic administration domain.

2. In the left pane, select **Security Realms**.

3. On the Summary of Security Realms page select the name of the realm (for example, `myrealm`).

4. On the Settings for Realm Name page select **Users and Groups** > **Users**.

5. Click **New** and provide the required information to create a user, such as `user1`, in the security realm.

6. Click the newly created user, `user1`.

**7.** Click the **Groups** tab.

**8.** Assign any of the groups with the `OAAM` prefix to the user, user1.

**9.** Click **Save**.

## 2.6 Importing the OAAM Snapshot

A full snapshot of policies, dependent components and configurations is shipped with Oracle Adaptive Access Manager. The `oaam_base_snapshot.zip` file is located in the *MW_HOME/IDM_ORACLE_HOME*/oaam/init directory.

**1.** Log in to the Oracle Adaptive Access Manager Administration Console (OAAM Admin) using the following URL:

```
http://host:port/oaam_admin
```

**2.** Load the snapshot file into the system by following these instructions:

**a.** Open **System Snapshot** under **Environment** in the Navigation tree.

**b.** Click the **Load from File** button.

A Load and Restore Snapshot dialog appears.

**c.** Deselect **Back up current system now** and click **Continue**.

A dialog appears with the message that you have not chosen to back up the current system, and do you want to continue?

**d.** When the dialog appears with the message that you have not chosen to back up the current system, and do you want to continue, click **Continue**.

The Load and Restore Snapshot page appears for you to choose a snapshot to load.

**e.** Browse for `oaam_base_snapshot.zip` and click the **Load** button to load the snapshot into the system database.

**f.** Click **OK** and then **Restore**.

The snapshot contains the following items that must be imported into OAAM:

- Challenge questions for English (United States)

  During registration, which could be enrollment, opening a new account, or another events such as a reset, the user selects different questions from a list of questions and enters answers to them. These questions, called challenge questions, are used to authenticate users.

  Questions for the languages you want to support must be in the system before users can be asked to register. These questions may also be required to log in to OAAM Server.

- Entity definitions

  The actors that are tracked during authentication are called authentication entities and include user, city, device, and so on. These base entities are required to enable conditions that are used for patterns.

- Out-of-the-box patterns

  Patterns are used by Oracle Adaptive Access Manager to either define one bucket or dynamically create buckets. Oracle Adaptive Access Manager collects data and populates these buckets with members based on pattern parameters, and rules

perform risk evaluations on dynamically changing membership and distributions of the buckets.

- Out-of-the-box configurable actions

  Configurable actions are actions that are triggered based on the result action or risk scoring or both after a checkpoint execution. The configurable actions are built using action templates.

  > **Note:** If you are upgrading from Oracle Adaptive Access Manager 10.1.4.5 to Oracle Adaptive Access Manager 11*g*, you see that the names and descriptions of the out-of-the-box action templates are slightly different, since the action templates in Oracle Adaptive Access Manager 11*g* are globalized and hence the difference.

- Out-of-the-box policies

  Policies are designed to help evaluate and handle business activities or potentially risky activities that are encountered in day-to-day operation.

- Any groups

  Collections of items used in rules, user groups, and action and alert groups are shipped with OAAM.

If you need to customize any properties, you should import the snapshot into your new test system, make the changes, export the snapshot, and import it into your new system. Alternatively you can import the snapshot on the new system and make the property changes directly, thereby eliminating the test system completely.

> **Note:** This procedure is only for first time initial setup. Importing a snapshot overwrites the existing environment and replaces it with a new one. For upgrades, import separate zip files for the entities, definitions, or policies.

For upgrading policies, components, and configurations, perform a backup, and then import the separate file. The following are available:

- Base policies are shipped in the `oaam_policies.zip` file, which is located in the *MW_HOME/IDM_ORACLE_HOME*/oaam/init directory

- Configurable action templates are shipped in the `OOTB_Configurable_Actions.zip` file, which is located in the *MW_HOME/IDM_ORACLE_HOME*/oaam/init directory.

- Base-authentication required entities are shipped in the `Auth_EntityDefinition.zip` file, which is located in the *MW_HOME/IDM_ORACLE_HOME*/oaam/init directory.

- Default patterns are shipped in the `OOB_Patterns.zip` file, which is located in the *MW_HOME/IDM_ORACLE_HOME*/oaam/init directory

## 2.7 Importing IP Location Data

IP location data is used by the risk policies framework to determine the risk of fraud associated with a given IP address (location).

To be able to determine location of the login or transaction, this data must be uploaded. For information, see Section 29.4, "Importing IP Location Data."

## 2.8 Enabling OTP

For information on enabling OTP, refer to Section 9.6, "Enabling OTP Challenge."

## 2.9 Setting the Time Zone Used for All Time Stamps in the Administration Console

A time zone identifies an area that always shares the same local time.

Time zones are used throughout Oracle Adaptive Access Manager for a variety of purposes. A time stamp can indicate when an alert was generated, the process start and end dates of a job, search pages, and so on. Users often are most comfortable working in their local time zones. As the administrator, you can configure the preferred time zones for the OAAM Administration Console.

The property is a system wide time zone setting and not a per-user one. All users must be in the single time zone.

Note that time zone and the browser locale formatting are independent of each other. For example, if you set your browser to `en-gb`, but set your `oaam.adf.time zone` to `America/Los_Angeles`, the time stamps are formatted as per British locale formatting but the time zone is still Pacific Time.

Use the Property Editor to set `oaam.adf.timezone` to the desired time zone.

For example,

`oaam.adf.timezone = Atlantic/Reykjavik`

For instructions on using the Properties Editor, refer to Chapter 28, "Using the Properties Editor."

The property takes the standard values for the time zone as listed in Section 2.9.1, "Values for the Common Timezones."

### 2.9.1 Values for the Common Timezones

The time zones are as follows:

Pacific/Midway (GMT-11:00) Midway - Samoa Time (ST)

Pacific/Pago_Pago (GMT-11:00) Pago Pago - Samoa Time (ST)

Pacific/Honolulu (GMT-10:00) Honolulu - Hawaii Time (HT)

America/Anchorage (GMT-09:00) Alaska Time (AKT)

America/Tijuana (GMT-08:00) Tijuana - Pacific Time (PT)

America/Vancouver (GMT-08:00) Vancouver - Pacific Time (Canada) (PT)

America/Los_Angeles (GMT-08:00) Los Angeles - Pacific Time (PT)

America/Chihuahua (GMT-07:00) Chihuahua - Mexico Time 2 (MT)

America/Denver (GMT-07:00) Denver - Mountain Time (MT)

America/Edmonton (GMT-07:00) Mountain Time

Canada (MT)

America/Phoenix (GMT-07:00) Mountain Time (MT)

America/Mazatlan (GMT-07:00) Mexico Time 2 (MT)

America/Guatemala (GMT-06:00) Guatemala - Central America Time (CT)

America/Regina (GMT-06:00) Regina - Central Time (CT)

America/Chicago (GMT-06:00) Chicago - Central Time (CT)

America/Managua (GMT-06:00) Managua - Central America Time (CT)

America/Winnipeg (GMT-06:00) Central Time (Canada) (CT)

America/El_Salvador (GMT-06:00) El Salvador - Central America Time (CT)

America/Costa_Rica (GMT-06:00) Costa Rica - Central America Time (CT)

America/Mexico_City (GMT-06:00) Mexico City - Mexico Time (MT)

America/Guayaquil (GMT-05:00) Guayaquil - Ecuador Time (ECT)

America/Indiana/Indianapolis (GMT-05:00) Indianapolis

Indiana - Eastern Time (ET)

America/Bogota (GMT-05:00) Bogota - Colombia Time (COT)

America/Lima (GMT-05:00) Lima - Peru Time (PET)

America/Panama (GMT-05:00) Panama - Eastern Time (ET)

America/Montreal (GMT-05:00) Montreal - Eastern Time (Canada) (ET)

America/New_York (GMT-05:00) New York - Eastern Time (ET)

America/Puerto_Rico (GMT-04:00) Puerto Rico - Atlantic Time (AT)

America/Halifax (GMT-04:00) Canada Atlantic Time (AT)

America/Santiago (GMT-04:00) Santiago - Chile Time (CLT)

America/Caracas (GMT-04:00) Caracas - Venezuela Time (VET)

America/Godthab (GMT-03:00) Godthab - Western Greenland Time (WGT)

America/Argentina/Buenos_Aires (GMT-03:00) Buenos Aires - Argentine Time (ART)

America/Sao_Paulo (GMT-03:00) Sao Paulo - Brasilia Time (BRT)

America/St_Johns (GMT-03:30) St Johns - Newfoundland Time (NT)

America/Noronha (GMT-02:00) Noronha - Fernando de Noronha Time (FNT)

Atlantic/Azores (GMT-01:00) Azores - Azores Time (AZOT)

Atlantic/Cape_Verde (GMT-01:00) Cape Verde - Cape Verde Time (CVT)

Europe/Dublin (GMT+00:00) Dublin - Greenwich Mean Time (GMT)

Europe/London (GMT+00:00) London - Greenwich Mean Time (GMT)

Etc/UTC (GMT+00:00) Coordinated Universal Time (UTC)

Africa/Casablanca (GMT+00:00) Casablanca - Western European Time (WET)

Europe/Lisbon (GMT+00:00) Lisbon - Western European Time (WET)

Africa/Nouakchott (GMT+00:00) Nouakchott - Greenwich Mean Time (GMT)

Atlantic/Reykjavik (GMT+00:00) Reykjavik - Greenwich Mean Time (GMT)

Europe/Prague (GMT+01:00) Prague - Central European Time (CET)

Europe/Budapest (GMT+01:00) Budapest - Central European Time (CET)

Europe/Madrid (GMT+01:00) Madrid - Central European Time (CET)

Europe/Vienna (GMT+01:00) Vienna - Central European Time (CET)

Africa/Algiers (GMT+01:00) Algiers - Central European Time (CET)

Africa/Lagos (GMT+01:00) Lagos - Western African Time (WAT)

Europe/Belgrade (GMT+01:00) Belgrade - Central European Time (CET)

Europe/Oslo (GMT+01:00) Oslo - Central European Time (CET)

Europe/Rome (GMT+01:00) Rome - Central European Time (CET)

Africa/Tunis (GMT+01:00) Tunis - Central European Time (CET)

Europe/Stockholm (GMT+01:00) Stockholm - Central European Time (CET)

Europe/Copenhagen (GMT+01:00) Copenhagen - Central European Time (CET)

Europe/Tirane (GMT+01:00) Tirane - Central European Time (CET)

Europe/Zurich (GMT+01:00) Zurich - Central European Time (CET)

Europe/Paris (GMT+01:00) Paris - Central European Time (CET)

Europe/Berlin (GMT+01:00) Berlin - Central European Time (CET)

Europe/Warsaw (GMT+01:00) Warsaw - Central European Time (CET)

Europe/Amsterdam (GMT+01:00) Amsterdam - Central European Time (CET)

Europe/Brussels (GMT+01:00) Brussels - Central European Time (CET)

Europe/Luxembourg (GMT+01:00) Luxembourg - Central European Time (CET)

Europe/Bucharest (GMT+02:00) Bucharest - Eastern European Time (EET)

Asia/Nicosia (GMT+02:00) Nicosia - Eastern European Time (EET)

Europe/Kiev (GMT+02:00) Kiev - Eastern European Time (EET)

Europe/Sofia (GMT+02:00) Sofia - Eastern European Time (EET)

Europe/Riga (GMT+02:00) Riga - Eastern European Time (EET)

Africa/Johannesburg (GMT+02:00) Johannesburg - South Africa Time (SAT)

Europe/Athens (GMT+02:00) Athens - Eastern European Time (EET)

Africa/Tripoli (GMT+02:00) Tripoli - Eastern European Time (EET)

Africa/Cairo (GMT+02:00) Cairo - Egypt Time (ET)

Asia/Beirut (GMT+02:00) Beirut - Eastern European Time (EET)

Europe/Tallinn (GMT+02:00) Tallinn - Eastern European Time (EET)

Europe/Vilnius (GMT+02:00) Vilnius - Eastern European Time (EET)

Europe/Helsinki (GMT+02:00) Helsinki - Eastern European Time (EET)

Asia/Amman (GMT+02:00) Amman - Eastern European Time (EET)

Asia/Damascus (GMT+02:00) Damascus - Eastern European Time (EET)

Africa/Harare (GMT+02:00) Harare - Central African Time (CAT)

Asia/Jerusalem (GMT+02:00) Jerusalem - Israel Time (IT)

Europe/Istanbul (GMT+02:00) Istanbul - Eastern European Time (EET)

Africa/Khartoum (GMT+03:00) Khartoum - Eastern African Time (EAT)

Asia/Aden (GMT+03:00) Aden - Arabia Time (AT)

Africa/Mogadishu (GMT+03:00) Mogadishu - Eastern African Time (EAT)

Asia/Baghdad (GMT+03:00) Baghdad - Arabia Time (AT)

Asia/Bahrain (GMT+03:00) Bahrain - Arabia Time (AT)

Africa/Djibouti (GMT+03:00) Djibouti - Eastern African Time (EAT)

Africa/Nairobi (GMT+03:00) Nairobi - Eastern African Time (EAT)

Europe/Moscow (GMT+03:00) Moscow - Moscow Time (MSK)

Asia/Qatar (GMT+03:00) Qatar - Arabia Time (AT)

Asia/Kuwait (GMT+03:00) Kuwait - Arabia Time (AT)

Asia/Riyadh (GMT+03:00) Riyadh - Arabia Time (AT)

Asia/Tehran (GMT+03:30) Tehran - Iran Time (IRT)

Asia/Dubai (GMT+04:00) Dubai - Gulf Time (GT)

Asia/Baku (GMT+04:00) Baku - Azerbaijan Time (AZT)

Asia/Muscat (GMT+04:00) Muscat - Gulf Time (GT)

Asia/Kabul (GMT+04:30) Kabul - Afghanistan Time (AFT)

Asia/Yekaterinburg (GMT+05:00) Yekaterinburg - Yekaterinburg Time (YEKT)

Asia/Karachi (GMT+05:00) Karachi - Pakistan Time (PKT)

Asia/Tashkent (GMT+05:00) Tashkent - Uzbekistan Time (UZT)

Asia/Kolkata (GMT+05:30) Kolkata - India Time (IT)

Asia/Colombo (GMT+05:30) Colombo - Sri Lanka Time (LKT)

Asia/Katmandu (GMT+05:45) Katmandu - Nepal Time (NPT)

Asia/Dhaka (GMT+06:00) Dhaka - Bangladesh Time (BDT)

Asia/Almaty (GMT+06:00) Almaty - Alma-Ata Time (ALMT)

Asia/Novosibirsk (GMT+06:00) Novosibirsk - Novosibirsk Time (NOVT)

Asia/Rangoon (GMT+06:30) Rangoon - Myanmar Time (MMT)

Asia/Krasnoyarsk (GMT+07:00) Krasnoyarsk - Krasnoyarsk Time (KRAT)

Asia/Ho_Chi_Minh (GMT+07:00) Ho Chi Minh - Indochina Time (ICT)

Asia/Jakarta (GMT+07:00) Jakarta - West Indonesia Time (WIT)

Asia/Bangkok (GMT+07:00) Bangkok - Indochina Time (ICT)

Asia/Kuala_Lumpur (GMT+08:00) Kuala Lumpur - Malaysia Time (MYT)

Asia/Shanghai (GMT+08:00) Shanghai - China Time (CT)

Asia/Taipei (GMT+08:00) Taipei - China Time (CT)

Asia/Irkutsk (GMT+08:00) Irkutsk - Irkutsk Time (IRKT)

Asia/Singapore (GMT+08:00) Singapore - Singapore Time (SGT)

Asia/Hong_Kong (GMT+08:00) Hong Kong - Hong Kong Time (HKT)

Asia/Manila (GMT+08:00) Manila - Philippines Time (PHT)

Australia/Perth (GMT+08:00) Perth - Western Time (Australia) (WT)

Asia/Yakutsk (GMT+09:00) Yakutsk - Yakutsk Time (YAKT)

Asia/Tokyo (GMT+09:00) Tokyo - Japan Time (JT)

Asia/Seoul (GMT+09:00) Seoul - Korea Time (KT)

Australia/Adelaide (GMT+09:30) Adelaide - Central Time (South Australia) (CT)

Australia/Darwin (GMT+09:30) Darwin - Central Time (Northern Territory) (CT)

Asia/Vladivostok (GMT+10:00) Vladivostok - Vladivostok Time (VLAT)

Pacific/Guam (GMT+10:00) Guam - Chamorro Time (ChT)

Australia/Hobart (GMT+10:00) Hobart - Eastern Time (Tasmania) (ET)

Australia/Sydney (GMT+10:00) Sydney - Eastern Time (New South Wales) (ET)

Australia/Brisbane (GMT+10:00) Brisbane - Eastern Time (Queensland) (ET)

Asia/Magadan (GMT+11:00) Magadan - Magadan Time (MAGT)

Pacific/Auckland (GMT+12:00) Auckland - New Zealand Time (NZT)

Pacific/Fiji (GMT+12:00) Fiji - Fiji Time (FJT)

Asia/Kamchatka (GMT+12:00) Kamchatka - Petropavlovsk-Kamchatski Time (PETT)

Etc/GMT-12 (GMT+12:00) Dateline Standard Time (UTC+12:00)

Pacific/Tongatapu (GMT+13:00) Tongatapu - Tonga Time (TOT)

# 3

# Oracle Adaptive Access Manager Navigation

OAAM Admin is a Web application that you can use to manage all environment, and Adaptive Strong Authenticator, and Adaptive Risk Manager features. Oracle Adaptive Access Manager 11*g* provides superior protection for businesses and their customers through strong yet easy-to-deploy multi-factor authentication and proactive, real-time fraud prevention.

This chapter describes the navigation panel, major nodes, and pages available in Oracle Adaptive Access Manager, and it also includes instructions on signing in to the application.

The chapter contains the following sections:

- Signing In to Oracle Adaptive Access Manager 11g
- OAAM Admin Console and Controls
- Navigation Panel
- Navigation Tree
- Policy Tree
- Management Pages
- Dashboard
- Online Help
- Search, Create, and Import
- Export to Excel
- Access Level to OAAM Admin

## 3.1 Signing In to Oracle Adaptive Access Manager 11*g*

This section describes how to sign in to OAAM Admin.

The features available when you sign in are based according to roles and business requirements.

An **Oracle Adaptive Access Manager Sign In** page is shown in Figure 3–1.

*Figure 3–1   Oracle Adaptive Access Manager Sign In*
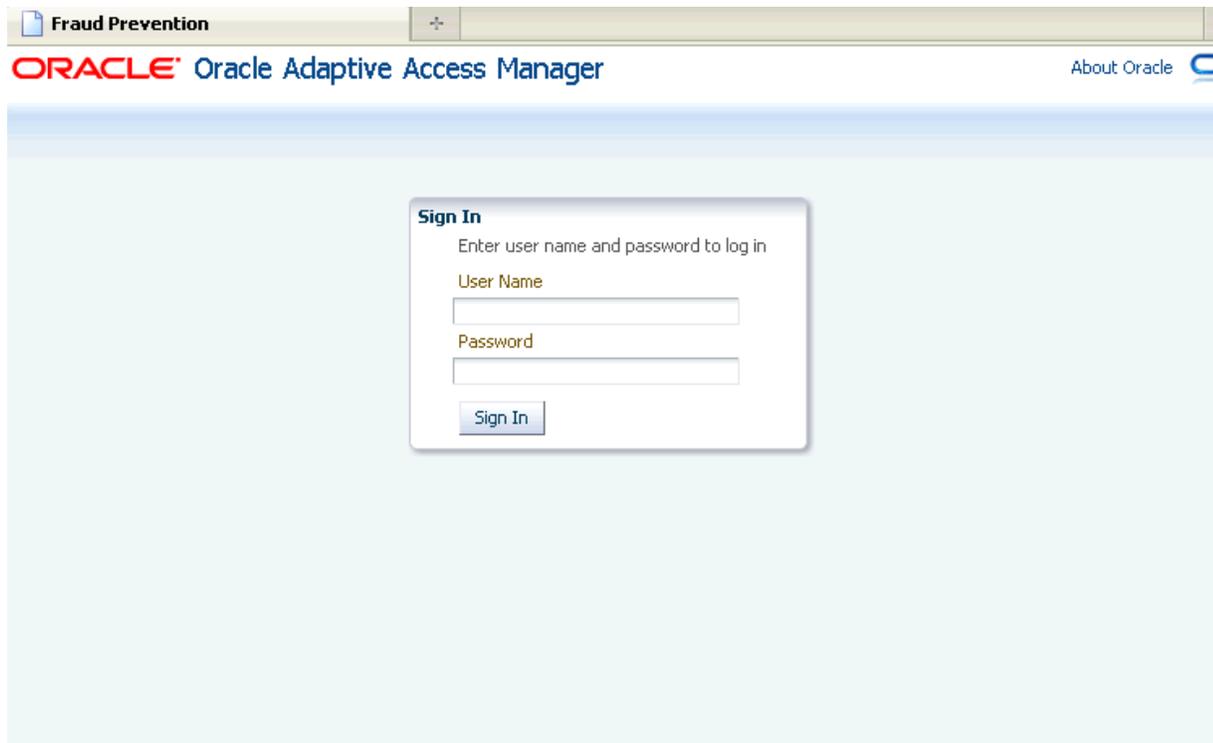


To sign in to OAAM Admin, follow these steps:

1.  In a browser window, enter the URL to the **Oracle Adaptive Access Manager 11g Sign In** page.

    ```
    http://host:port/oaam_admin/
    ```

    where

    - *host* refers to the Oracle Adaptive Access Manager managed server host

    - *port* refers to the OAAM Admin managed server port

    - `/oaam_admin/` refers to the OAAM Admin Sign In page

2.  On the **Sign In** page, enter your credentials.

3.  Click the **Sign In** button.

    If you have logged in successfully, the **Fraud Prevention** tab appears on the left with an expanded navigation tree.

To sign out, select the **Sign Out** link in the upper-right corner of OAAM Admin.

## 3.2  OAAM Admin Console and Controls

Upon a successful sign in, Oracle Adaptive Access Manager displays the OAAM Admin Console.

The Console is divided into the following areas: navigation panel on the left and the main, active page on the right.

The navigation panel helps users access all environment, Adaptive Strong Authenticator, and Adaptive Risk Manager features of Oracle Adaptive Access Manager. Named nodes in the panel identifies these items.

Initially, no active page is opened on the right side of OAAM Admin. You must open a node first.

Figure 3–2 shows OAAM Admin with an active page opened.

*Figure 3–2    OAAM Admin Console*
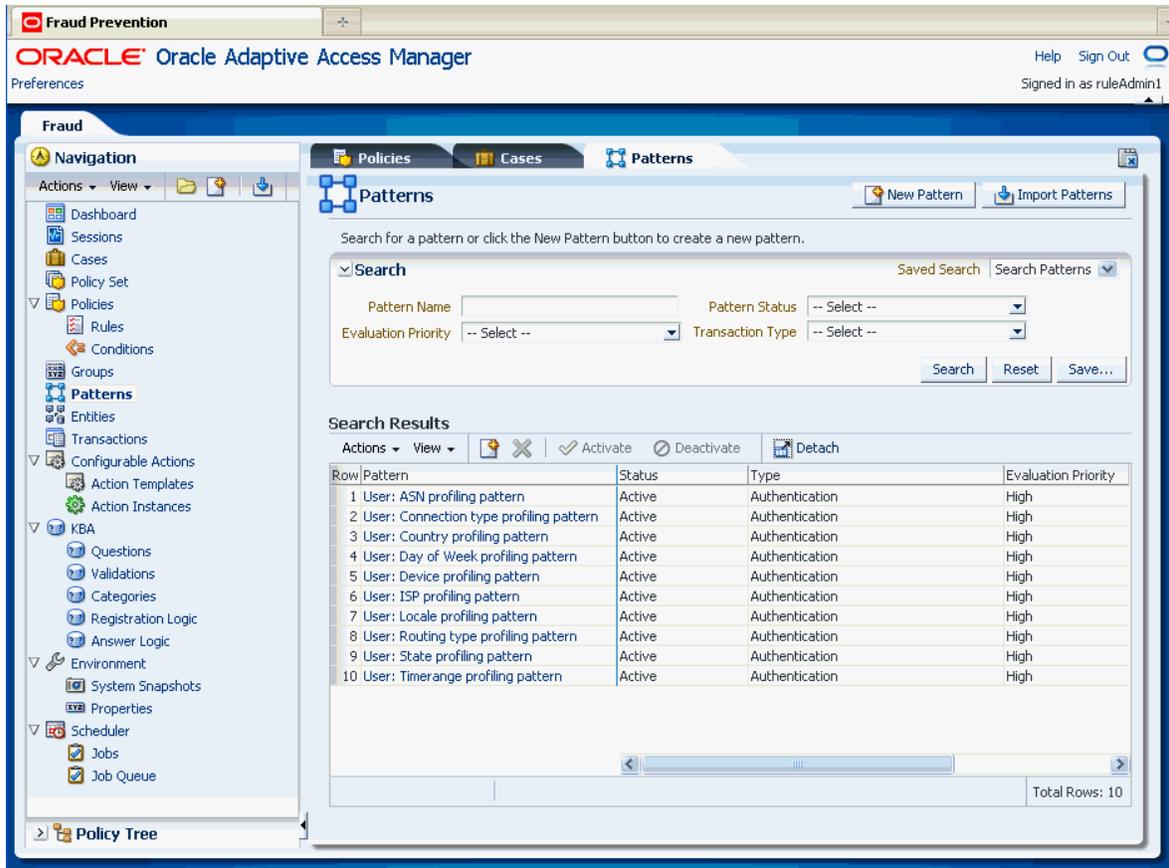


When you open a node, a new tab opens with the corresponding details or search page. A named tab identifies each open page. The active page generally enables you to create, view, and modify items.

You can have up to ten pages open at one time, which enables multitasking.

---

**Note:**   If you try to open more than ten tabs, an error appears with the message that only ten tabs are allowed to be kept open. You can manually close one or more tabs and then try to open the new tab.

---

When multiple pages are open, only the active page and named tabs of other open pages are visible. You can click a named tab to return to the corresponding page.

The following sections provide more information about OAAM Admin:

- Navigation Panel

- Navigation Tree

- Policy Tree

- Management Pages

■ Online Help

## 3.3 Navigation Panel

OAAM Admin provides navigators for easy access to different features of Oracle Adaptive Access Manager.

The Navigation panel in OAAM Admin contains the following trees:

■ Navigation Tree

■ Policy Tree

## 3.4 Navigation Tree

The Navigation tree, illustrated in Figure 3–3, is a collapsible and expandable tree that provides quick and visible access to features of Oracle Adaptive Access Manager.

### 3.4.1 Navigation Tree Structure

The Navigation tree includes named nodes that identify the individual features and groups of items within the Oracle Adaptive Access Manager product on which you can take action.

Figure 3–3 illustrates the Navigation tree.

*Figure 3–3   Navigation tree*



Depending on your access level, the Navigation tree can display the following nodes:

*Table 3–1    OAAM Features*

| Features | Function |
| --- | --- |
| Dashboard | Access feature, which provides a high-level view of real customer data. |
| Cases | Access tools for creating and supporting Customer Service Representative (CSR). Cases not available in offline. |
| Policies | Access feature for designing policies to evaluate and handle business activities or potentially risky activities |
| Groups | Access feature to create groups for simplifying workload. |
| Sessions | Access feature to view the forensic record of a session |
| Patterns | Access feature to create patterns used for profiling behavior |
| Entities | Access feature to create data structure, which comprises of a set of attributes, that can be re-used across different transactions. |
| Transactions | Access feature to create transaction definitions so that client-specific transactions and parameters can be captured for monitoring |
| KBA | Access framework to manage tasks that impact challenge questions, validations and levels of logic algorithms used for answers, question categories, and levels of logic algorithms used for registration. |
| Scheduler | Access feature to manage jobs. |
| Environment | Access feature to manage Oracle Adaptive Access Manager environment. |
| Configurable Actions | Access feature to create custom actions |

## 3.4.2  Navigation Tree Menu and Toolbar

A menu and toolbar appears above the Navigation tree, as shown Figure 3–3. Menus provide commands that you can use to take action on the selected item in the Navigation tree. Many menu commands are also provided as command buttons in the toolbar for quick access.

*Figure 3–4    Menu and Toolbar*



**Create New**



**Create New** opens the corresponding create page of the selected node. **Create New** is available only for certain nodes where applicable. See Table 3–2, " Create New of Selected Nodes" for a list of pages that can be opened by clicking **Create New**.

*Table 3–2    Create New of Selected Nodes*

| Node | Subnode | Create Page or Dialog |
| --- | --- | --- |
| Dashboard | | N/A |
| Sessions | | Not available |
| Cases | | Create Case |
| Policy Sets | | Not available |
| Policies | | New Policy |
| | Rules | Not available |
| | Conditions | Not available |
| Groups | | Create Group |
| Patterns | | New Pattern |
| Entities | | New Entity |
| Transactions | | New Transaction |
| Configurable Actions | | |
| | Action Templates | New Action Template |
| | Action Instances | New Action Instance |
| KBA | | Not available |
| | Questions | New Questions |
| | Validations | Not Available |
| | Categories | New Category |
| | Registration Logic | Not available |
| | Answer Logic | Not available |
| Scheduler | | Not available |
| | Jobs | Jobs search |
| | Job Queue | Job Queue |
| Environment | | Not available |
| | Snapshots | Not available |
| | Properties | New Property |

**Open**



**Open** opens the corresponding page for the node you have selected.

**Import**



**Import** opens the Import dialog for the node you have selected.

**View Menu**

Figure 3–5, "View Menu" illustrates the **View** menu and commands. Menu items that cannot be used on the selection in the Navigation tree appear in grey.

*Figure 3–5   View Menu*
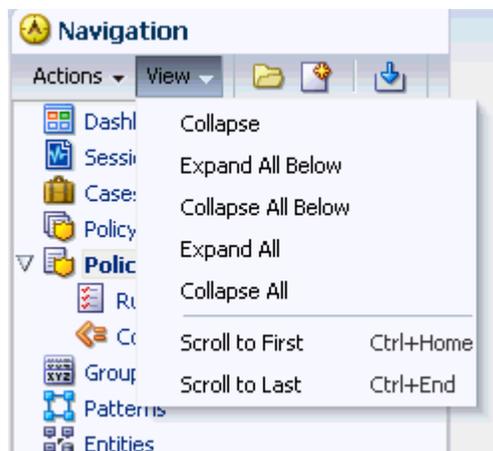


The **View** menu command descriptions are provided in Figure 3–3.

*Table 3–3    View Menu Commands*

| Command | Description |
| --- | --- |
| Collapse | Immediately closes the node. |
| Expand All Below | Immediately reveals all items below the selection. |
| Collapse All Below | Immediately closes the node and all items below the selection. |
| Expand All | Immediately reveals all the nodes and subnodes along with their leaf nodes in the Navigation tree. |
| Collapse All | Immediately closes all the nodes and subnodes along with their leaf nodes in the Navigation tree. |
| Scroll to First | Scrolls to the first node |
| Scroll to Last | Scrolls to the last node |

**Actions Menu**

Figure 3–6 illustrates the **Actions** menu, which provides appropriate commands for the selection in the Navigation tree. For instance, if you have **Policies** selected in the Navigation tree, one of the commands, **New Policy...**, on the **Actions** menu enables you to open the **New Policy** page for creating a new policy.

*Figure 3–6   Action Menu*



*Table 3–4    Actions Commands*

| Command | Description |
| --- | --- |
| Open | Opens the search or details page for the selected item in the Navigation tree. |
| List | Opens the item, search, or details page. |
| New | Activates a new page that you can fill in to define a new item. |
| Import | Displays the Import dialog, which enables you to locate and import the item. |

## 3.5  Policy Tree

The Policy tree gives a visual representation of the policy hierarchy and the relationship between different policies, user groups, and the checkpoints.

Double-clicking an item in the Policy tree opens a dynamic tab for that item. This enables administrators to view and edit the configurations in context.

You can expand the Policy tree to view the details about the user groups and policies under each checkpoint.

For example the **Forgot Password** policy is under the **Forgot Policy Checkpoint** and **All Users** is assigned to the policy.

*Figure 3–7   Policy Tree*
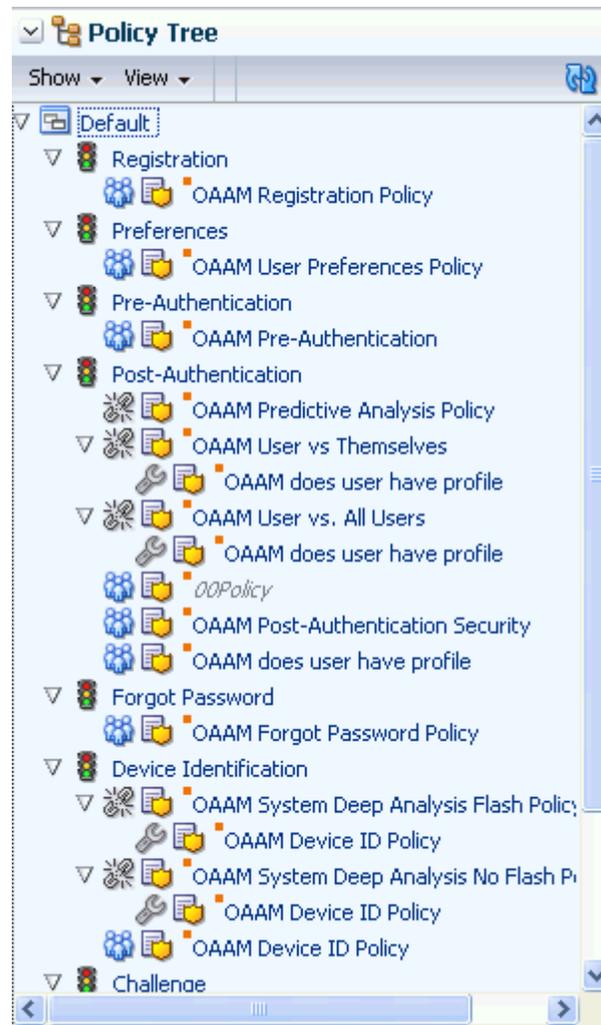


Policy is the last level in the Policy tree. You cannot drill down further except to see nested policies.

Table 3–5 provides a legend for the icons which appear on the Policy tree.

*Table 3–5    Policy Tree Legend*

| Icon | Definition | Description |
|------|-----------|-------------|
|  | Checkpoint | The checkpoint is a decision and enforcement point when policies are call to run their rules. |

**Table 3–5   (Cont.) Policy Tree Legend**

| Icon | Definition | Description |
|------|-----------|-------------|
| | Policy | The policies available in the system. |
| | | Disabled policies are grayed out. |
| | | Policies linked to multiple user groups are bolded and highlighted. |
| | | To open the **Policy Details** page of a policy, double-click the **Policy** node. The **Policy Details** page can also be opened by clicking **Open Selected** from the context menu. |
| | | To view nested policies, expand the policy node. |
| | All Users | Policy is linked to **All Users**. |
| | User Groups | Policy is linked to **Users** |
| | No user group | No users are associated with the policy. |
| | Trigger combination | Trigger combinations exist in the policy. |
| | More... | Summary information is available about the policy. |

From the Policy tree, you can click the **More** icon for summary information on the policy.
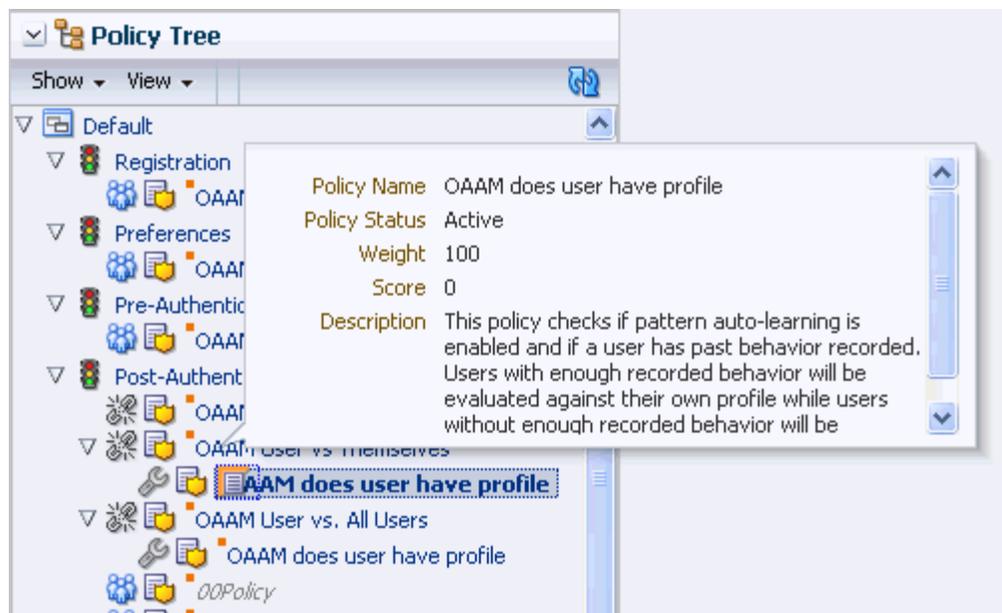
## 3.6 Management Pages

The individual features and groups of items are organized on the Navigation tree. To open a component, double-click its node in the Navigation tree. The details of that node or a search page opens in a new tab on the right side of the console. A named tab identifies each open page, like the tabs on manila folders.

Only the active page is visible, with as many named tabs of other open pages that can fit on one line. You can click a named tab to return to the corresponding page.

The nodes and their corresponding pages are listed in Table 3–6.

*Table 3–6 Open Pages*

| Node | Subnode | Pages |
| --- | --- | --- |
| Dashboard | | Dashboard |
| Sessions | | Sessions |
| Cases | | Cases search page |
| Policy Sets | | Policy Sets page |
| Policies | | Policies search page |
| | Rules | Rules search page |
| | Conditions | Conditions search page |
| Groups | | Groups search page |
| Patterns | | Pattern search page |
| Entities | | Entities search page |
| Transactions | | Transactions search page |
| Configurable Actions | | Not available |
| | Action Templates | Action Templates search page |
| | Action Instances | Action Instance search page |

*Table 3–6   (Cont.)  Open Pages*

| Node | Subnode | Pages |
| --- | --- | --- |
| KBA | | Not available |
| | | Note: KBA is not available in offline mode. |
| | Questions | Questions search page |
| | Validations | Validations search page |
| | Categories | Categories search page |
| | Registration Logic | Registration Logic page |
| | Answer Logic | Answer Logic page |
| Environment | | Not available |
| | System Snapshot | Snapshots search page |
| | Properties | Properties search page |
| Scheduler | | |
| | Jobs | New Job |
| | Job Queue | |

## 3.6.1  Search Pages

The search page is the starting place for managing the environment, adaptive strong authentication, and adaptive risk management features, and groups of like items.

You can open a search page by:

- Double-clicking a node in the Navigation tree

- Right-clicking a node in the Navigation tree and selecting the **List** command from the context menu that appears

- Selecting the node in the Navigation tree and then choosing the **List** command from the **Actions** menu

When a search page first appears, you see a search filter and a **Search Results** table. The **Search Results** table is initially empty. You must click the **Search** button to see a list of items.

To search for items:

1. Select the criteria to search from the pull-down lists. The lists of available criteria varies according to the feature.

2. Enter strings to match in the text boxes.

3. Select or specify filters to narrow the search scope.

4. Click the **Search** button to trigger the search and to display the results in the Search Results table.

The search returns all items that match the specified criteria; leave the fields empty to obtain the list of all items of the type.

### 3.6.1.1  Elements in the Search Form

This section describes the elements in the search forms.

**Search**

You can search for items using the attribute search criteria fields.

**Reset**

The **Reset** button enables you to reset the search criteria.

**Saved Searches**

You can create saved searches that persist for the duration of your session. You would enter the search criteria, then click the **Save** button to open the **Personalize Saved Search** dialog. The **Personalize Saved Search** dialog is used to specify how you want to save the search criteria you entered. You can name the search, for example, **myspecialsearch**, so that it displays in the **Saved Search** list.



### 3.6.1.2 Search Results Table

The Search Results table shows at most the first 200 matches found by the search.

You can sort the results by using the **Sort Ascending** and **Sort Descending** buttons next to the column name.



If the description of an item is too long to be fully shown, positioning the cursor over the visible text displays the entire description.
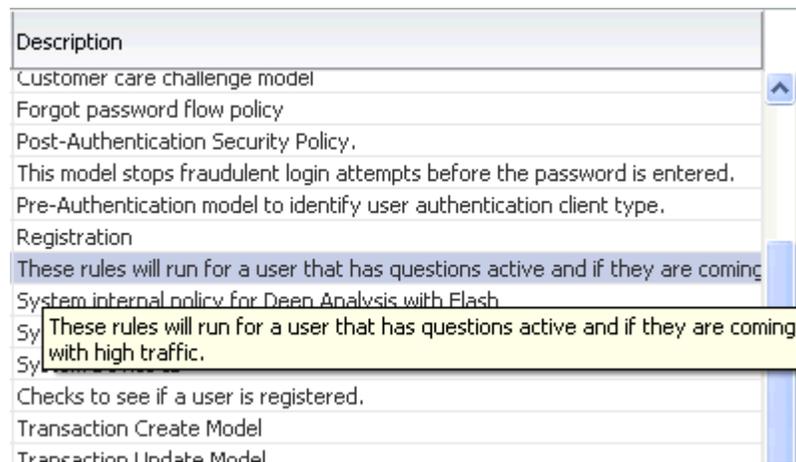
Once an item is selected in the **Search Results** table, an action can be performed on it by clicking one of the icons on the toolbar or by selecting a command from the **Actions** menu.

If you want to see more details, click the available link for the item.

### 3.6.1.3 Search Results Menu and Toolbar

A menu and toolbar appears above the **Search Results** table. Figure 3–8 shows the **Search Results Menu and Toolbar** from the **Patterns Search** page.

*Figure 3–8 Results Menu and Toolbar*
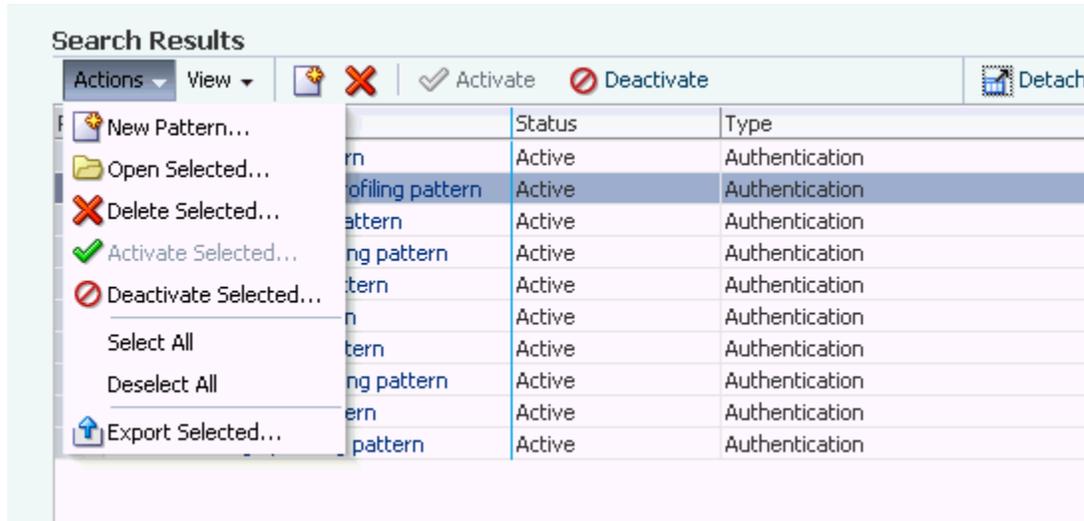


The **Actions** menu and command buttons provide appropriate commands for the selection in the Navigation tree and **Search Results** table.

Figure 3–8 shows command buttons that may be available, depending on the selection.

*Table 3–7 Results Menu and Toolbar*

| Button | Definition | Description |
|---|---|---|
| | Create | Opens a new page, which you can fill in to add a new item of the selected type. The new page opens as the active page on the right side of the Navigation tree. |
| | Delete | Removes the selected item. |
| | Create Like | Creates a new item that is similar— or "like"—the existing one. |

*Table 3–7 (Cont.) Results Menu and Toolbar*

| Button | Definition | Description |
|---|---|---|
| | Activate | Activates the selected item. |
| | Deactivate | Deactivates the selected item. |
| | Detach | Detaches the Results table. |

### 3.6.1.4  Select All

You can select all the results to perform actions on by clicking the header of the Row column in the upper-left corner of the **Search Results** table.
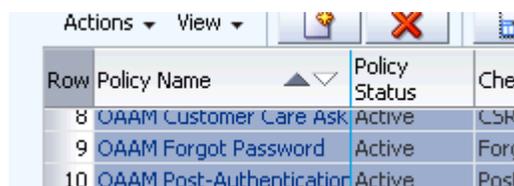


### 3.6.1.5  Create and Import

Generally, buttons to create new items or import items are in the upper-right corner of the console.



### 3.6.1.6  Close Multiple Tabs

The small close tabs button in the upper-right corner of the console enables you to close the tabs you are viewing.



If you have multiple tabs open, a Close Multiple Tabs dialog appears. To close multiple tabs, highlight the names of the tabs, and press **OK**.
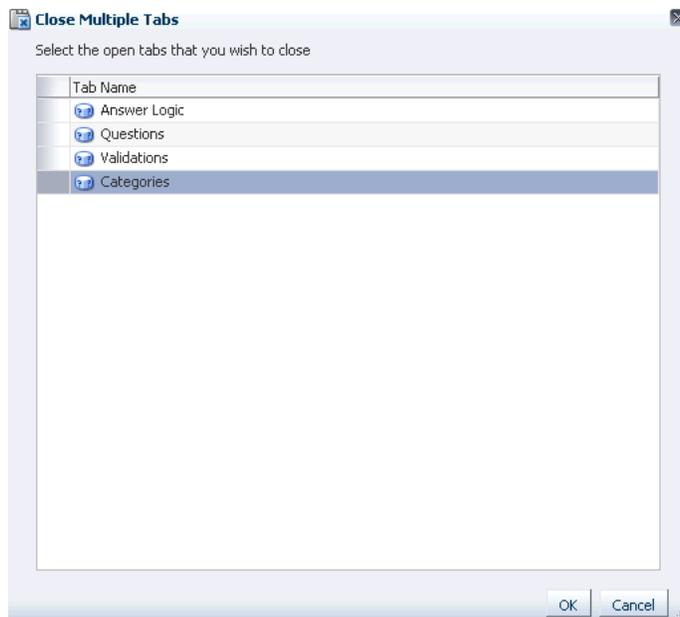
## 3.6.2  Detail Pages

You can view details of a specific item by opening its details page.

A **Case Details** page is shown in Figure 3–9.

**Figure 3–9    Case Details**

## 3.7 Dashboard

The dashboard presents a real-time view of activity via aggregates and trending.

The dashboard is divided into three sections:

- The performance panel (Section 1) presents real-time 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 (Section 2) presents aggregate data based on time range and different data types.

- The dashboard panel (Section 3) presents historical data. The detailed dashboards are used for trending data over time ranges.

## 3.8 Online Help

To access online help documentation, on the upper right corner of any window, click **Help** to bring up the help window. A help topic for the relevant top-level search or details page is displayed. These help topics contain links to information in an online version of the *Oracle Fusion Middleware Administrator's Guide for Adaptive Access Manager*.

Selecting **Managing Oracle Adaptive Access Manager 11g Online Help** displays several topics in the online documentation.

Topics that are displayed by selecting **Help** appear in only English and Japanese languages. Online Help is not translated into the nine Admin languages.

Refer to the following illustration for an example of an online help window.
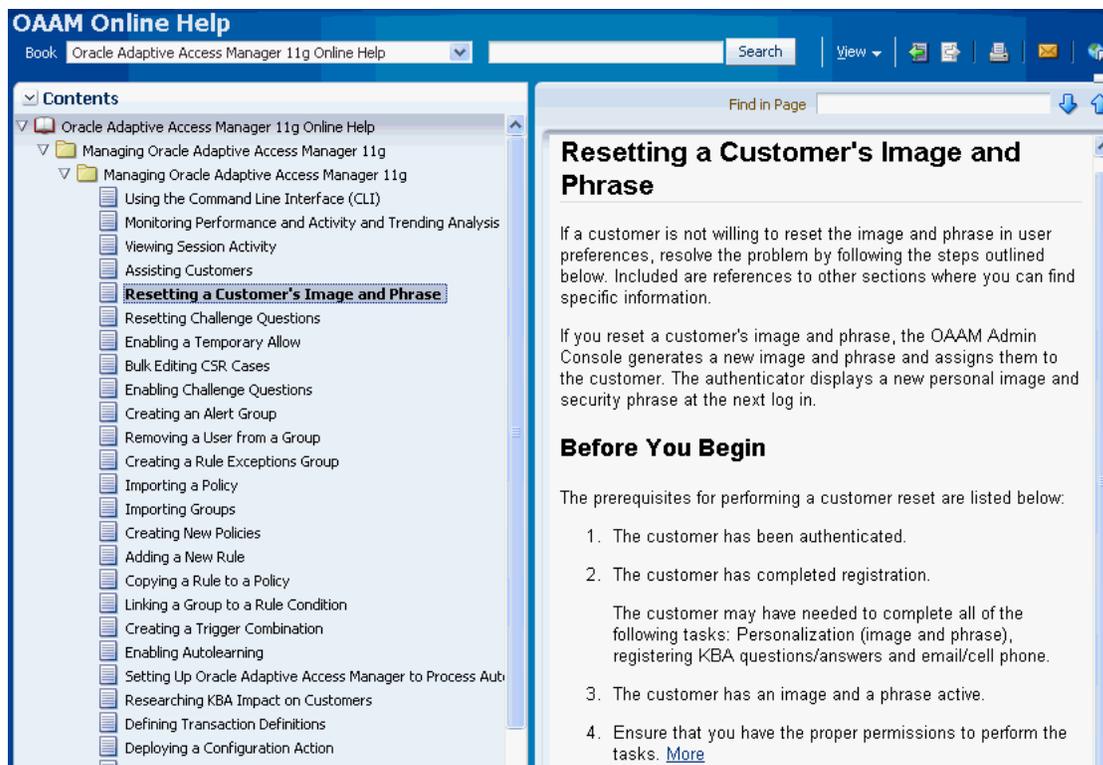
## 3.9 Search, Create, and Import

Oracle Adaptive Access Manager provides more than one way to search, create, and import.

**Search**

Depending on the selection, you can open a **Search** page by:

- Double-clicking the node in the Navigation tree.
- Right-clicking the node in the Navigation tree and selecting **List <item>** from the context menu.
- Selecting the node in the Navigation tree and then choosing **List <item>** from the **Actions** menu.
- Clicking the **List <item>** button in the Navigation tree toolbar.

**Create**

Depending on the selection, you can open a **Create** page by:

- Clicking the **New <item>** button in the upper right of the console.
- Right-clicking the node in the Navigation tree and selecting **New <item>** from the context menu.
- Selecting the node in the Navigation tree and then choosing **New <item>** from the **Actions** menu.
- Clicking the **Create new <items>** button in the Navigation tree toolbar.
- Selecting the **Create New <item>** button from the **Search Results** toolbar.
- Selecting **New <item>** from the **Actions** menu in **Search Results**.

**Import**

Depending on the selection, you can open a **Import** page by:

- Clicking the **Import <item>** button in the upper right of the console.
- Right-clicking the node in the Navigation tree and selecting **Import <item>** from the context menu.
- Selecting the node in the Navigation tree and then choosing **Import <item>** from the **Actions** menu.
- Clicking the **Import <items>** button in the Navigation tree toolbar.

## 3.10 Export to Excel

You can generate a report of the results from the Search pages for policies, questions, validations, snapshots, properties, entities, transactions, conditions, groups, patterns, and so on.

To export results to an Excel report:

1. Ensure the oaam.export.max.rows.allowed property is configured so that you are able to export all the rows needed. This property limits the maximum row selection.

2. In a search page, select rows the rows of interest from the search results.

3. Click the **Export To Excel** button.

When the export confirmation dialog is shown, you can view the selected list. The export table with the selected rows shows the ID number and display name columns, so that you can easily identity and verify the selected rows before the export.

4. Click **Export** to export the rows to Excel.

## 3.11 Access Level to OAAM Admin

OAAM Admin provides functions for security investigators and customer service representatives (CSRs), business and security analysts, security administrators, system administrators, and quality assurance. The functions and navigation that are available depend on the roles.

Refer to Table 3–8 for conceptual roles. These example roles are for reference only and do not refer to official OAAM out-of-the-box roles.

For information on the Navigation and Policy trees, see Section 3.4, "Navigation Tree" and Section 3.5, "Policy Tree."

*Table 3–8    Access Level*

| Oracle Adaptive Access Manager Conceptual Roles | Descriptions | Access |
|---|---|---|
| Security investigators and customer service representatives (CSR) | Security investigators and customer service representatives (CSR) use Oracle Adaptive Access Manager's case management tools to handle security and customers cases daily. They have detailed knowledge about user activity and security issues. | Customer support representatives can search, open and create CSR type cases. They do not have any access to the Navigation tree.<br><br>Security investigators have wide access to OAAM Admin. |
| Security administrators | Security administrators plan, configure and deploy policies based on the requirements from analysts. | Security administrators configure such items as policy set, patterns, rules, groups, and so on. They do not have access to environment properties, system snapshots, or the OAAM dashboard, and view-only access to cases.<br><br>They can access the Navigation tree. |
| Business and security analysts | Analysts gather intelligence from various sources to identify business and security needs and develop requirements to address them. Their sources for intelligence include investigators, industry reports, antifraud networks, compliance mandates, and company policies.<br><br>Analysts work with security investigators and CSRs to identify the policies that require adjustment and new policies that must be created. | Business analysts do not have access to environment properties and system snapshots. They have read-only access the Navigation tree and cases. |
| System administrator | A system administrator configures environment-level properties and transactions. | System administrators have limited access to OAAM Admin to manage the server environment and Scheduler: Jobs/Scheduler: Job Queue. The server environment includes logging, properties, and enumerations. |
| QA | QA tests the policies to confirm that they meet requirements. | QA have access to all the functionality. |

Oracle Adaptive Access Manager 11*g* users must be defined using the Oracle WebLogic Administration Console.

For information on defining Oracle Adaptive Access Manager users, see the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

# Part II

## Customer Service and Forensics

This part of the book presents information about the customer service and forensics tools of Oracle Adaptive Access Manager.

It contains the following chapters:

- Chapter 4, "Managing and Supporting CSR Cases"
- Chapter 5, "Investigation Using Agent Cases"
- Chapter 6, "Viewing Additional Details for Investigation"

# 4

# Managing and Supporting CSR Cases

Oracle Adaptive Access Manager provides a set of tools for creating and supporting Customer Service Representatives (CSR) cases. This chapter provides information to CSR and CSR Managers for managing cases and contains the following sections:

- Introduction and Concepts
- CSR and CSR Manager Role Permissions
- Getting Started
- Cases Search Page
- Case Details Page
- Viewing Case Activity
- Viewing Customer's Sessions
- Creating a CSR Case
- Performing Customer Resets
- Performing Challenge Question Resets
- Enabling a Temporary Allow
- Performing Case Actions
- Configuring Expiry Behavior for CSR Cases
- Reporting
- Multitenancy
- Use Cases
- Best Practices and Recommendations

## 4.1 Introduction and Concepts

This section provides an introduction to CSRs and CSR Managers and a high-level view of how they might use the Oracle Adaptive Access Manager set of tools for creating and supporting cases. It includes the following sections:

- Case
- Customer Service Representative (CSR)
- CSR Manager
- Fraud Investigator

- [Fraud Investigation Manager](#)

- [Locked Status](#)

- [Temporary Allow](#)

- [Case Status](#)

- [Severity Level](#)

- [Expiration Date](#)

- [Customer Resets](#)

### 4.1.1 Case

A **case** is a record of all the actions performed by the CSR to assist the customer as well as various account activities of the customer. Each case is allocated a **case number**, a unique case identification number. The Case Management feature of Oracle Adaptive Access Manager is used in two ways.

- Users of the enterprise using Oracle Adaptive Access Manager can call up the enterprise asking for assistance with user-facing features of Oracle Adaptive Access Manager such as images, phrases or challenge questions, or any issues with their account. The CSR uses the Case Management feature to create a case which records all the actions performed by the CSR to assist the user as well as various account activities of the user.

- The Case Management feature is also used by Fraud Investigators to investigate potentially fraudulent activity performed in user accounts.

#### 4.1.1.1 CSR Cases

**CSR cases** are used in customer service situations associated within the normal course of doing business online and over the phone when providing assistance to customers. A CSR case is created for a specific user.

#### 4.1.1.2 Escalated Cases

CSR escalates a case when he cannot resolve a case and needs further investigation by an investigator or when he determines there is suspicious activity associated with the specific user and he wants further investigation by an investigator. Once escalated the case is treated as an Agent case, which is no longer visible to the CSR. However, any agent can work on the escalated case.

### 4.1.2 Customer Service Representative (CSR)

**Customer service representatives** are employed by many different types of companies to serve as a point of contact for customers who call. They are responsible for ensuring that their company's customers receive an adequate level of service and help for low risk issues originating from customer calls. In handling customers' complaints, they must attempt to resolve the problem according to guidelines established by the company. These procedures may involve opening a case, entering notes as they are speaking to customers, asking questions to determine the validity of a complaint, making changes or updates to a customer's profile information, and, if required, passing the case on to a CSR Manager who has the appropriate privileges to respond. In a Multitenant deployment, CSRs only have access to cases limited to an Organization.

### 4.1.3 CSR Manager

The **CSR Manager** is in charge of overall management of CSR-type cases. A CSR Manager has all the access and responsibilities of a CSR and access to more operations, such as:

- bulk edit cases

- temp allow users

- extend expiration

The CSR does not have the permissions to perform these actions. A CSR Manager routinely searches through the CSR cases to check on status and clean up if needed.

### 4.1.4 Fraud Investigator

A **Fraud Investigator** investigates a specific fraud scenario or suspicious pattern. The Fraud Investigator works on escalated cases.

### 4.1.5 Fraud Investigation Manager

A **Fraud Investigation Manager** has access to actions that the Fraud Investigator does not have.

### 4.1.6 Locked Status

If the user fails a challenge, he is locked out of the account. The status of the account is **Locked**. The Locked status is only used if the **Knowledge Based Authentication (KBA)** or **One Time Password (OTP)** facility is in use.

- Knowledge Based Authentication (KBA): For online challenges, a customer is locked out of the session after the Online Counter reaches the maximum number of failures. For phone challenges, a customer is locked out when the maximum number of failures is reached and no challenge questions are left.

- One Time Password: OTP sends a single-use password to the user through a configured delivery method, and if the user exceeds the number of retries when attempting to put in his OTP code, his account becomes locked.

After the lock out, a CSR must reset the status to **Unlocked** before the account can be used to enter the system.

### 4.1.7 Temporary Allow

A temporary allow grants temporary account access to a customer who is being blocked from logging in or performing a transaction. A customer is blocked when a security rule is triggered. For example, a customer may be traveling on business and attempting to log in from a blacklisted country and the system has blocked him or her.

### 4.1.8 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. CSRs cannot Authentication a closed case. CSR Managers and Investigators can Authentication a closed case. Escalated cases cannot be created.

### 4.1.9 Severity Level

The **Severity Level** is a marker to communicate to case personnel how serious the case is. The severity level is set by whomever creates the case. The available severity levels are **High**, **Medium**, and **Low**.

### 4.1.10 Expiration Date

---

**Note:** Depending on the type of the case, the terminology used and behavior may be different.

---

The **expiration date** is the date when a case expires. By default, the length of time before a case expires is 24 hours, but is configurable.

- **CSR cases**: For CSR cases, the status of the case changes from the current status to **Expired**. The case could have any status when it expires. The CSR can open the case but cannot perform any actions on it. The CSR Manager can extend an expired case.

- **Escalated cases**: For escalated cases, the status of the case changes from the current status to **Expired**. When the case is expired, an expired flag is set for the case to let managers know that the case requires their attention. For example, if escalated cases are set to 24 hours and if the case is open and has not been accessed in more than 24 hours, the flag is set to **Expired**. When the Fraud Investigator accesses the expired case, it is reactivated and the expiration date is extended for another 24 hours (or however long it has been configured for). The expired behavior is configurable using the Properties Editor. CSRs cannot change the expiration date of escalated cases.

  For information, refer to Section 4.13, "Configuring Expiry Behavior for CSR Cases."

### 4.1.11 Customer Resets

Oracle Adaptive Access Manager uses images and phrases on virtual authentication devices as part of the personalization to help prevent fraud. The Customer Resets feature enables you to reset the customer's image and phrase and unregister his device. The Customer Reset feature is not be available for a closed, an escalated or an expired case.

## 4.2 CSR and CSR Manager Role Permissions

Customer Service personnel can access various functionality in Oracle Adaptive Access Manager based on the role to they are assigned. The out-of-box roles are CSR and CSR Manager. A CSR has limited access to the OAAM Administration Console. Their primary function is to resolve low risk customer issues originating from customer calls.

A CSR Manager has all the access and responsibilities of a CSR and access to more sensitive operations. The CSR Manager is in charge of the overall management of CSR type cases.

*Table 4–1    CSR and CSR Manager Role Permissions*

| Action | CSR Permissions | CSR Manager Permissions |
| --- | --- | --- |
| Search Cases | Search for CSR cases | Search for CSR cases |
| | Search for open and closed cases. | Search for open and closed cases. |
| New Case | Create only CSR cases | Create only CSR cases |
| View Case Details | View closed case details | View closed case details |
| | View Transactions in Sessions tab (CSRs do not have access to Session details from Queries) | View Transactions in Sessions tab |
| Edit Case | Add notes to closed cases (view only for everything else) | Authentication closed cases |
| | Perform all customer and KBA resets on a CSR case | Add notes to CSR cases |
| | Perform KBA phone challenge on a CSR case | Change status and severity on a CSR case |
| | Change status and severity on a CSR case | Bulk edit CSR cases |
| | | Temp allow users |
| | | Extend expiration |
| | | Perform all customer and KBA resets |
| | | Perform KBA phone challenge |

## 4.3  Getting Started

Before using the case tools, read through Section 4.1, "Introduction and Concepts"—the section is useful in helping you to understand the concepts presented in this chapter. To perform the operations listed earlier, log in as a CSR or CSR Manager. When you log in, you are redirected to the **Cases Search** page; CSRs do not have access to other applications (Navigation tree and Policy tree).

If you have the appropriate permissions, you can open to the **Cases Search** page by double-clicking **Cases** in the Navigation tree. Alternatively, you can open the **Cases Search** page by:

- Right-clicking **Cases** in the Navigation tree and selecting **List Cases** from the context menu.

- Selecting **Cases** in the Navigation tree and then choosing **List Cases** from the **Actions** menu.

- Clicking the **List Cases** button in the Navigation tree toolbar.

The **Cases Search** page is the starting place for managing CSR cases. From the **Cases Search** page, you can:

- create new cases

- create like cases

- bulk edit cases

- perform searches

If you are a CSR, you can open only one case at a time. CSR Managers, Investigators, and Investigation Managers can open multiple case tabs.

## 4.4 Cases Search Page

The **Cases Search** page contains the search tools to help you find cases that you are interested in. An example **Cases Search** page is shown in Figure 4–1.

*Figure 4–1   CSR Cases Search page*



### 4.4.1 Searching for Cases

When a customer telephones with a question or problem, you can search all customers and cases quickly through any combination of factors. For example, you can search for a customer's open case by entering his User ID and **New**, **Pending**, and **Escalated** for his case status. Another example is searching for CSR cases created between a month ago and yesterday.

To search cases:

1. From the **Cases Search** page, specify criteria in the Search Filter.

   The filters are shown in Table 4–2.

*Table 4–2   Search Filters*

| Filter | Description |
|---|---|
| Organization ID | To locate cases for an organization, select the Organization ID. |
| | In a Multitenant deployment, CSRs only have access to cases limited to an Organization. Organization names to which the user has access are presented. |
| User Name | To locate cases for a specific user, enter his user name or part of a user name in the User Name field. |
| User ID | To locate a case by the user identifier. |
| Case ID | To locate a specific case, enter the Case ID. |
| Description Keyword | To locate a case by a keyword that is in the description, enter the word you want. |
| Case Type | To filter cases by case type, select CSR. |

*Table 4–2   (Cont.)  Search Filters*

| Filter | Description |
| --- | --- |
| Severity Level | To filter cases by severity level, select Low, High, or Medium. |
| Case Status | To filter cases by case status, select New, Pending, Closed, Escalated. |
| Expired | To filer the list by expired, select the option you want. |
| | The options available are: |
| | ■  Hide Expired |
| | ■  Show Only Expired |
| Created Date | To locates cases created within a given create date range, enter the start and end dates you want for the range. |
| Disposition | To filter cases by dispositions, you can select: |
| | ■  Confirmed Fraud |
| | ■  Duplicate |
| | ■  False Negative |
| | ■  False Positive |
| | ■  Issue Pending |
| | ■  Issue Resolved |
| | ■  Not Fraud |
| | The disposition describes the way in which the issue was resolved in a case. Cases only have dispositions when they are closed. If a case has any status besides closed, the disposition is left blank. |
| Last Action | Search based on the last action that was taken in case. |
| Notes | Search for cases that contain specific keywords in their log. For example, if you search for all cases that contain the word "chargeback," a case with a note that contains "The device used seems to be related to a number of chargebacks" would return in the list of cases. |
| Created by | Search by user name of the agent who created the case. |
| Current Owner | Search by user name of the agent who is working on this case currently (who performed the last action) |

**2.**  Click **Search**.

There is a link on the case number. To view the case details, click the link. You can get the case detail for cases that belonged to any user belonging to the group you have access to. If the user does not belong to the group you have access to, you do not see that case in search results.

## 4.4.2  Viewing a List of Cases

Depending on the criteria entered for the search, the **Search Results** table can display a list of cases. In a multitenant environment, if the user does not belong to an organization you have access to, you do not have access to his case. If you had been assigned to one organization previously and created cases for users in that organization and serviced them, when you are reassigned to another organization, you only see cases for the new organization when you log in again, regardless of whether you serviced them or not.

### 4.4.3 Viewing a List Cases You are Currently Working On

From the **Cases Search** page, enter your user name in the Current Owner field to locate cases that you are currently working on and click **Search**. The Search Results table displays the list of cases you are currently working on.

### 4.4.4 Searching for Open and Closed Cases

1. From the **Cases Search** page, search by **Case Status**:

   - **New**, **Pending**, and **Escalated** to locate open cases

   - **Closed** to locate closed cases

   For information, see Section 4.4.1, "Searching for Cases."

2. Click the case number of the case you want.

   The **Case Details** page is displayed (Figure 4–2).

   When the CSR or CSR Manager opens the case

   - The current owner becomes the CSR or CSR Manager.

   - The Created By field remains the same.

   - The status of the case is "Pending."

3. Next, the CSR or CSR Manager can perform the necessary actions such as granting a temporary allow, performing challenge question resets, and other actions.

### 4.4.5 Searching Case by Description Keyword

Searching by description keywords would display all cases with any matching words in that was entered as a description during case creation.

1. From the **Cases Search** page, enter the description keyword to locate cases that contains the **Description Keyword** and click **Search**.

2. Click the case number of the case you want.

   The **Case Details** page appears (Figure 4–2).

### 4.4.6 Viewing a List of Cases

Searching by description keywords would display all cases with any matching words that was entered as a description during case creation.

## 4.5 Case Details Page

By clicking the case number on the **Cases Search** page, you can review the details of a specific case perform various actions on cases. The **Case Details** page provides such general details about the case as the customer's user name, status, severity level, and description. For information, see Section 4.5, "Case Details Page."

*Figure 4–2   Case Details*



## 4.5.1  Case Actions

**Case Details** also provides access to the actions that can be taken, a log of case activity, and a list of customer sessions. From the **Case Details** page, the following options are available:

- Add Notes
- Ask Question
- Customer Resets
- Temporary Allow (CSR Manager Only)
- Change Severity
- Change Status
- Extend Expiration Date (CSR Manager Only)
- Escalate Case (CSR Manager Only)

You can only act on those case that you can access in the details page. You can open the case only when you have access to the user's group.

## 4.5.2 Viewing Case Details

The following information is displayed in **Case Details**.

- **Case Status** - The current state of a case. Status values used for the case are **New**, **Pending**, **Escalated**, or **Closed**.

- **Severity Level** - The available severity levels are **High**, **Medium**, and **Low**. For information about severity levels, see Section 4.1.9, "Severity Level."

- **Description** - The details for the case. A description is required.

- **Case Created** - The date and time the case was created.

- **Last Case Action** - The last action executed 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 in all CSR cases. Escalated cases are not taken into account.

- **Date of Last Global Case Action** - The last action performed against the user online.

- **Expiration Date (for CSR cases)** - The date when a case expires. For information about expiration dates, see Section 4.1.10, "Expiration Date."

- **Disposition** - The description of how the issue was resolved when the case was closed. Cases only have dispositions when they are closed. If a case has any status besides closed, the disposition is left blank.

## 4.5.3 Viewing User Details

The following information is displayed in **User Details**.

- **User Name** - Identifier a user uses to log in

- **Organization ID** - The unique identifier for the organization the user belongs in

  The combination of **User Name** and **Organization ID** is the unique identifier for a user accessing an application. In a multitenant deployment, CSRs only have access to cases limited to an Organization.

- **Completed Registration** - If the user has completed registration, this field shows **Yes**; otherwise it shows **No**. To be registered a user may need to complete all of the following tasks: Personalization (image and phrase), registering challenge questions/answers and email/cellphone.

- **Personalization Active** - When the 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**.

- **Questions Active** - If user has completed registration, but questions have been reset, and the user has not 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 or she can be challenged.

- **OTP Active** - If supported OTP delivery channels are registered, the field shows **Yes**.

- **Last Online Action** - The last action that the user executed. For example, **Block** is displayed if the user is blocked.

- **Date of Last Online Action** - The date when the last online action was executed.

- **Temporary Allow Active** - If temporary allow is active, this field shows **Yes**; otherwise the field shows **No**.

- **Temporary Allow Expiration Date** - When temporary allow is enabled; this field tells you when it expires. If temporary allow is 7 days, the expiry date is a week from today.

## 4.6 Viewing Case Activity

OAAM Admin maintains a unique log of every customer service action taken while working on a case. The log is available in the **Logs** tab of the **Case Details** page. Each log entry includes the Log ID, User ID of the CSR, create date, action, subaction, and notes. You can use this log while you are on the phone with a customer to view the case history.

*Figure 4–3    Logs Tab*



### 4.6.1 Viewing the Case History

To view the case history:

1. From the **Cases Search** page, specify criteria in the Search Filter.

   For information, see Section 4.4.1, "Searching for Cases."

**2.** Click the case number of the case you want.

View the activity log for that case (Figure 4–3).

## 4.6.2 Searching the Log of a Case

To search the log of a case:

**1.** Display the log for the case you want to search, as described in Section 4.6.1, "Viewing the Case History."

**2.** Enter the search criteria and click **Search**.

*Table 4–3    Log Search Filters*

| Filter | Description |
| --- | --- |
| Notes Keyword | Keyword in notes describing why an action was taken in a case. For example, suspected fraud. |
| ARM ID | The type of agent that performed the action. For example, csrm1 |
| Created Date | The date of the case action. |
| Action | The action taken for the case. For example, escalation. |

## 4.6.3 Viewing Escalated Case Logs and Notes

To view the log and notes of an escalated case:

**1.** In the **Cases Search** page, search by the case status and by other filters to locate the case.

For example, search for **Agent** cases for Alex's user name. For information, see Section 4.4.1, "Searching for Cases."

**2.** Click the case number of the case you want.

The **Case Details** page appears (Figure 4–2).

**3.** Click the **Log** tab.

The activity log for that case appears.

**4.** Enter the search criteria and click **Search**.

# 4.7 Viewing Customer's Sessions

OAAM Admin maintains a history of a customer's sessions. Each session entry includes the Session ID, authentication status, login time, Device ID, location, transactions, and alerts. Sessions information is available in the **Sessions** tab of the **Case Details** page. You can use the **Sessions** tab while you are on the phone with a customer to view the sessions history (a list of that customer's previous sessions).

**Figure 4–4   Sessions Tab**



## 4.7.1 Viewing a Customer's Session History

To view a customer's session history:

1. From the **Cases Search** page, specify criteria in the Search Filter.

   For information, see Section 4.4.1, "Searching for Cases."

2. Click the case number of the case you want.

   The **Case Details** page appears.

3. Click the **Sessions** tab (Figure 4–4).

## 4.7.2 Searching for a Customer's Sessions

To search for a customer's sessions:

1. Display the list of sessions for the case, as described in Section 4.7.1, "Viewing a Customer's Session History."

2. Enter search criteria and click **Search**.

*Table 4–4    Sessions Search Filters*

| Filter | Description |
| --- | --- |
| Session ID | The identifier for the session. For example, 11702. |
| Device ID | The identifier for the device. For example, 1803. |
| Auth Status | The authentication status. For example, Success. |
| Alert Level | The alert level. For example, Info |
| Transactions | The transaction performed. |
| Login Time | The time the customer logged in to perform the transaction. For example, 5/11/09. |

You can search sessions belonging to the users that belong to the organizations that you have access to.

### 4.7.3 Searching for a Customer's Sessions by Device ID or Date Range

To search for a customer's sessions by Device ID or date range:

1. Display the list of sessions for the case, as described in Section 4.7.1, "Viewing a Customer's Session History."

2. To search the sessions by **Device ID**, enter the ID of the device.

3. To search the sessions by login date range, click the calendar icons and select the start date and the end date.

4. Click **Search**.

### 4.7.4 Filtering the Session History by Authentication Status or Alert Level

To filter the list of customer's sessions by authentication status or alert level

1. Display the list of sessions for the case, as described in Section 4.7.1, "Viewing a Customer's Session History."

2. To filter the sessions by authentication status, select the authentication status you want.

3. To filter the sessions by alert level, select the alert level you want.

4. Click **Search**.

### 4.7.5 Viewing Transactions in the Sessions History

To view the customer's transactions.

1. Display the list of sessions for the case, as described in Section 4.7.1, "Viewing a Customer's Session History."

2. Filter the log by transactions.

3. Click **Search**.

## 4.8 Creating a 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 CSR while assisting a customer. Procedures are described in this section for creating new and like cases.

### 4.8.1 Creating a Case

The CSR is only able to create cases for users of the organizations he has permissions for. A new CSR case is created by a CSR Manager or CSR when a customer care situation occurs either online or through a phone call. The CSR or CSR Manager searches for cases by the Organizations ID and user name.

In a Multitenant deployment, CSRs only have access to cases limited to an Organization. He is not be able to see the case if the user belongs to an organization he does not have permission for.

Depending on the case, the CSR or CSR Manager decides if a new case must be created or if it can be handled with an existing case for that user.

To create a new case:

1. In the **Cases Search** page, click **New Case**.

   The **Create Case** screen appears.

   You could also open the **Create Case** screen by right-clicking **Cases** in the Navigation tree and selecting **New Case** from the context menu that appears.

*Figure 4–5   Create Case*



2. Select the **Organization ID**.

   A list of **Organization ID**s for which you have access to is provided. From the list you can select one **Organization ID**.

   You can select an **Organization ID** and enter a **user name** or enter the **User ID**.

3. Enter the **user name**.

   User name is the identifier a user uses to log in. The combination of **user name** and **Organization ID** is the unique identifier for a user accessing an application. The unique **Organization ID** and **user name** combination must be available in the system. The user name is case-sensitive. If the user name is invalid or does not use

the correct uppercase and lowercase, an error message appears when you press **Create**.

4.  Enter the **User ID**.

    **User ID** is unique identifier generated by the system for the user.

5.  Select a severity level from the **Severity Level** list

    The available severity levels are **High**, **Medium**, and **Low**.

6.  Enter a description in the **Description** field, or select a description from the **Canned Description** list, or both.

    **Description** is a required field. You can select multiple descriptions from the **Canned Description** list for the same case, one at a time for any number of times. Each description selected from the list is appended to the previous description. If you are entering a description, the **Description** field can contain alphanumeric and special characters.

7.  Click **Create** or **Cancel**.

    The **Create** button is disabled until all the fields are entered. No fields can be left blank.

    If an invalid parameters were entered, an error message is displayed and the new case is not created. If you click **Cancel**, the **Cases Search** page appears. If you click **Create**, a new case is created, and you are directed to the **Case Details** page of the newly created case.

    When the **Case Details** page is displayed:

    -   The **Case Status** shows **Pending**.

    -   The **Created By** field shows the user name of the CSR who created the case.

    -   The **Current Owner** field shows his user name because he is the current owner of the case.

## 4.8.2 Creating a Case Like Another Case

To create a new case that is similar— or "like"—an existing case:

1.  From the **Cases Search** page, select a case by clicking in the checkbox next to case in the **Search Results** table.

2.  Click the **Create Like** button.

    The **Create Like** button is disabled if you select multiple rows in the **Search Results** table. The **Create Case Like** screen appears with pre-populated data from the original case. If you had chosen a closed case, the **Create Case Like** screen shows pre-populated data from the case except the **Case Status** is **New**.

    If you had chosen an escalated case, the **Create Like** screen shows pre-populated data from the case except the **Case Status** is **New** and the **Case Type** is **CSR**.

*Figure 4–6   Create Like*



3.  Enter a description in the **Description** field, or select a description from the **Canned Description** list, or both.

    **Description** is a required field. You can select multiple descriptions from the **Canned Description** list for the same case, one at a time for any number of times. Each description selected from the list is appended to the previous description. If you are entering a description, the **Description** field can contain alphanumeric and special characters.

4.  Edit any of the other fields if you want.

    Do not leave any fields blank.

5.  Click **Create** or **Cancel**.

    If you click **Cancel**, the **Cases Search** page appears. If you click **Create**, a new case is created with data from the original case and your changes, and you are directed to the **Case Details** page of the newly created case.

## 4.9  Performing Customer Resets

Authenticator uses images and phrases on its virtual authentication devices as part of the personalization to help prevent fraud. **Customer Resets** enable you to reset the customer's image and phrase and unregister his device. **Customer Resets** are not be available for a closed, escalated or expired case.

### 4.9.1  Resetting Image

If you reset a customer's image, OAAM Admin randomly assigns a new image to the customer. After resetting the image, you can inform the customer that the authenticator will display a new image at the next log in to the Web site. The same phrase will continue to be used. If a customer is not registered and does not have an image to reset, an error message appears if you try to reset his image.

To reset a customer's image:

1. From the **Cases Search** page, search for an existing case for resetting the image for the customer, and if it does exist, click the case number in the results table.

2. If the case does not exist, create one for resetting the customer's image.

3. On the menu bar of the Case Details page, click **Customer Resets**.

   The **Customer Resets** screen is displayed.

*Figure 4–7 Customer Resets*



4. In the **User Item** list, select **Image**.

5. In the **Canned Notes** list, select the note you want to add.

6. Edit the note describing why you are taking the action, if necessary.

7. Click **Submit**.

## 4.9.2 Resetting Phrase

When the customer's phrase is reset, a new one is randomly assigned to the customer. After resetting the phrase, you can inform the customer that the authenticator will display a new phrase the next time he or she logs in to the Web site. The same image will continue to be used.

To reset a customer's phrase:

1. From the **Cases Search** page, search for an existing case for resetting the phrase for the customer, and if it does exist, click the case number in the results table.

2. If the case does not exist, create one for resetting the customer's phrase.

3. On the menu bar of the Case Details page, click **Customer Resets**.

   The **Customer Resets** screen is displayed.

4. In the **User Item** list, select **Phrase**.

5. In the **Canned Notes** list, select the note you want to add.

6. Edit the default notes in the **Notes** field.

7. Click **Submit**.

   An error message appears if the customer is not registered and does not have a phrase to reset.

### 4.9.3 Resetting Image and Phrase

If you reset a customer's image and phrase, OAAM Admin generates a new image and phrase and assigns them to the customer. Afterward, you can inform the customer that the authenticator will display a new personal image and phrase at the next log in to the Web site.

To reset a customer's image and phrase:

1. From the **Cases Search** page, search for an existing case for resetting the image and phrase for the customer, and if it does exist, click the case number in the results table.

2. If the case does not exist, create one for resetting the customer's image and phrase.

3. On the menu bar of the Case Details page, click **Customer Resets**.

   The **Customer Resets** screen is displayed.

4. In the **User Item** list, select **Image and Phrase**.

5. In the **Canned Notes** list, select the note you want to add.

6. Edit the default notes in the **Notes** field.

7. Click **Submit**.

   An error message appears if the customer is not registered and does not have a phrase and an image to reset.

### 4.9.4 Unregistering Devices

When you unregister devices, OAAM Admin unregisters all of a customer's devices. The customer can register another device if he wants.

To unregister a customer's devices:

1. From the **Cases Search** page, search for an existing case for unregistering the device for the customer, and if it does exist, click the case number in the results table.

2. If the case does not exist, create one for unregistering the customer's device.

3. On the menu bar of the Case Details page, click **Customer Resets**.

   The **Customer Resets** screen is displayed.

4. In the **User Item** list, select **Unregister Devices**.

5. In the **Canned Notes** list, select the note you want to add.

6. Edit the default notes in the **Notes** field.

7. Click **Submit**.

### 4.9.5 Resetting OTP Profile

When a customer's OTP profile is reset, the system deletes the contact information that is used to send the OTP. Out of the box, the user is asked to register contact information on next login, if the OTP profile is reset. OAAM deployments may choose to use both KBA and OTP. If that is the case, if the OTP profile is reset, but questions are still active, the customer is asked to reregister OTP information at the next login.

To reset a customer's OTP profile:

1. From the **Cases Search** page, search for an existing case for resetting the OTP profile for the customer, and if it does exist, click the case number in the results table.

2. If the case does not exist, create one for resetting the customer's OTP profile.

3. On the menu bar of the Case Details page, click **Customer Resets**.

   The **Customer Resets** screen is displayed.

4. In the **User Item** list, select **Reset OTP profile**.

5. In the **Canned Notes** list, select the note you want to add.

6. Edit the default notes in the **Notes** field.

7. Click **Submit**.

#### OTP Delivery Method Reset Example

Jacob calls the CSR and requests that his OTP delivery method be reset and change from phone to SMS and provides a phone number for SMS.

Carl the CSR performs these steps:

1. Carl searches for Jacob's logins and verifies with him about last login time and place.

2. Carl creates a case for Jacob and resets his OTP delivery method.

3. He asks Jacob to login again and verify the new OTP delivery method.

4. After he is done and confirms the new OTP working fine, Carl goes ahead and closes the case.

### 4.9.6 Resetting Virtual Authentication Device

A customer may sometimes ask to have the virtual authentication device reset.

To reset a customer's virtual authentication device:

1. From the **Cases Search** page, search for an existing case for resetting the virtual authentication device for the customer, and if it does exist, click the case number in the results table.

2. If the case does not exist, create one for resetting the customer's virtual authentication device.

3. On the menu bar of the Case Details page, click **Customer Resets**.

   The **Customer Resets** screen is displayed.

4. In the **User Item** list, select **Reset Authentication Pad**.

5. In the **Canned Notes** list, select the note you want to add.

6. Edit the default notes in the **Notes** field.

**7.** Click **Submit**.

### 4.9.7 Unlocking OTP

The CSR unlocks the customer who calls because he or she has been OTP-locked. Unlocking the customer resets the customer's OTP failure counter to 0.

To unlock OTP for the customer:

**1.** From the **Cases Search** page, search for an existing case for unlocking the OTP for the customer, and if it does exist, click the case number in the results table.

**2.** If the case does not exist, create one for unlocking the customer's OTP.

**3.** On the menu bar of the Case Details page, click **Customer Resets**.

The **Customer Resets** screen is displayed.

**4.** In the **User Item** list, select **Unlock OTP**.

**5.** In the **Canned Notes** list, select the note you want to add.

**6.** Edit the default notes in the Notes field.

**7.** Click **Submit**.

### 4.9.8 Resetting All Registration Data, Challenge Counters, and OTP Contact and Delivery Information

The **Customer (All)** option resets all user registration information including security phrase, image, challenge questions, challenge (question and OTP) counters, and OTP profile.

To reset all registration data, challenge counters, and OTP profile information:

**1.** From the **Cases Search** page, search for an existing case for resetting all registration data, challenge counters, and OTP contact and delivery information for the customer, and if it does exist, click the case number in the results table.

**2.** If the case does not exist, create one for the customer.

**3.** On the menu bar of the Case Details page, click **Customer Resets**.

The **Customer Resets** screen is displayed.

**4.** In the **User Item** list, select **Customer (All)**.

**5.** In the **Canned Notes** list, click the note you want to add.

**6.** Edit the default notes in the **Notes** field.

**7.** Click **Submit**.

## 4.10 Performing Challenge Question Resets

Authenticator uses questions as additional credentials to help prevent fraud. You can perform question-related actions for the customer when necessary. The Challenge Questions feature enables you to reset the following items for a customer:

- Reset Questions
- Next Question
- Reset Question Set
- Unlock Customer

- Ask Question

### 4.10.1 Performing Challenge Questions Related Actions

Open the **Challenge Questions** screen by following these instructions:

1. From the **Cases Search** page, search for an existing case for performing the reset for the customer, and if it does exist, click the case number in the results table.

2. If the case does not exist, create one for the customer.

3. On the menu bar of the Case Details page, select **More Actions**, and then click **Challenge Questions**.

   The **Challenge Questions** screen appears.

*Figure 4–8   Challenge Questions*



### 4.10.2 Resetting Challenge Questions

Resetting challenge questions deletes the existing questions and answers and generates a new question set for the customer to register from. The customer is informed that registration of challenge questions (select new questions and answers from his or her question set) is required at the next log in to the Web site.

To reset a customer's challenge questions:

1. Open the **Challenge Questions** screen, as described in Section 4.10.1, "Performing Challenge Questions Related Actions."

2. In the **Item** list, select **Reset Questions**.

3. In the **Canned Notes** list, select the note you want to add.

   For example, you could select the **Forgot Question/Answers**.

4. Click **Submit**.

   After completing the task, you can enter a note about the actions that were taken (Section 4.12.1, "Adding Notes to Cases") and change the status of the case if necessary (Section 4.12.3, "Changing Status of a Case").

**Question Reset Example**

Martha calls the CSR and requests that her questions be reset since she has forgotten answers to her challenge questions.

Carl the CSR performs these steps:

1. Carl searches for Martha's logins and verifies with her about last login time and place.

2. Carl creates a case for Martha and resets her questions.

3. He asks Martha to login again and register the questions.

4. After she is done and confirms the new questions are registered, Carl goes ahead and closes the case.

### 4.10.3 Resetting Challenge Questions and the Question Set

Resetting the challenge question set resets the challenge questions and the question set that the customer can register questions from. The customer is informed that registration of challenge questions is required at the next log in to the Web site.

To reset a customer's challenge questions and the set of questions to pick from:

1. Open the **Challenge Questions** screen, as described in Section 4.10.1, "Performing Challenge Questions Related Actions."

2. In the **Item** list, select **Reset Question Set**.

3. In the **Canned Notes** list, select the note you want to add.

4. Click **Submit**.

   After completing the task, you can enter a note about the actions that were taken (Section 4.12.1, "Adding Notes to Cases") and change the status of the case if necessary (Section 4.12.3, "Changing Status of a Case").

### 4.10.4 Incrementing a Customer to His Next Question

If you reset the customer's next question, OAAM Admin advances the customer to the next challenge question in his list of registered questions. So if he is currently being asked question A, he is now asked question B or C. The customer is informed that he will be asked a different challenge question the next time he logs in to the Web site.

To increment a customer to his next question:

1. Open the **Challenge Questions** screen, as described in Section 4.10.1, "Performing Challenge Questions Related Actions."

2. In the **Item** list, select **Next Question**.

3. In the **Canned Notes** list, select the note you want to add.

4. Click **Submit**.

   After completing the task, you can enter a note about the actions that were taken (Section 4.12.1, "Adding Notes to Cases") and change the status of the case if necessary (Section 4.12.3, "Changing Status of a Case").

### 4.10.5 Unlocking a Customer (KBA)

When you unlock a customer, he or she is forced to register new questions and answers the next time he successfully logs in.

To unlock the customer:

1. Open the **Challenge Questions** screen, as described in Section 4.10.1, "Performing Challenge Questions Related Actions."

2. In the **Item** list, select **Unlock Customer**.

3. In the **Canned Notes** list, select the note you want to add.

4. Click **Submit**.

   After unlocking the user you can close the case if desired (Section 4.12.3, "Changing Status of a Case").

## 4.10.6 Performing KBA Phone Challenge

Users can be authenticated over the phone using their registered challenge questions. This option is not available for unregistered users or in deployments not using KBA.

To use a customer's challenge questions for phone authentication:

1. Open the **Challenge Questions** screen, as described in Section 4.10.1, "Performing Challenge Questions Related Actions."

2. In the **Item** list, select **Ask Question**.

3. In the **Canned Notes** list, select **User Challenged**.

   If you select **User Challenged**, the **Notes** field contains the phrase, **Request for customer question**, which you can edit to describe why you are taking the action.

4. Click **Submit**.

5. In the confirmation dialog, click **OK**.

   The **Ask Question** screen appears displaying a challenge question to ask the customer and a field to enter customer's response.

6. Ask the customer the question.

7. Enter the customer's answer in the **Answer** field.

8. Click **Submit**.

   Failure counters are used to lock out fraudsters so that they are unable to obtain the answers/questions.

   The maximum number of questions the user is allotted is 3 by default. The maximum number of attempts per question is 3 by default for phone challenges. In phone challenges the CSR enters the user's answers for him. If you enter an incorrect answer for the user, left the field blank, or closed the screen for the user, the failure counter is incremented. The same challenge question remains on the screen until the maximum number of attempts per question is reached. Then, another question is displayed.

   Since the customer is given three attempts per question, a maximum of nine attempts is allowed for the phone challenge. If a question is answered correctly, the failure counter is reset and the system automatically takes appropriate actions depending on the status such as unlocking the customer. If the customer does not provide correct answers and exceeds the maximum number of failures, he is locked out.

*Figure 4–9   Ask Question Flow*
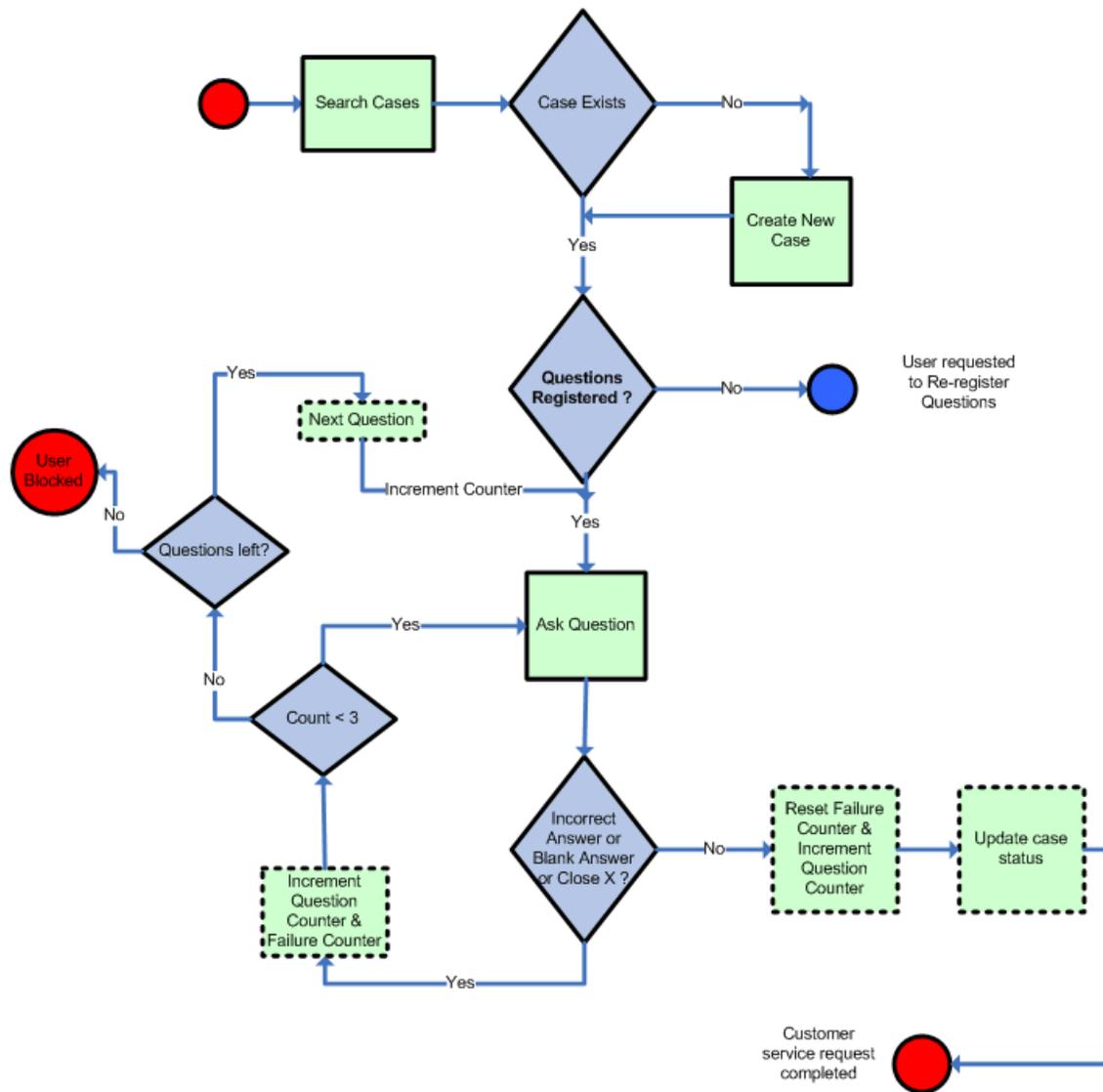


### Ask Questions Example

1. Log in as a CSR and create a case for the customer and ask KBA questions through using the Ask Question case action.

   Enter the user's answers until he answers correctly or is locked out.

2. If the user answers the question correctly, inform the user he must register new questions online next time he logs in.

3. Verify reset questions works for user after asking challenge questions.

   You need to actually verify this by doing logins before and after the reset action to verify that the user is asked to register.

## 4.11  Enabling a Temporary Allow

To enable a temporary allow:

1. From the **Cases Search** page, search for an existing case for granting a temporary allow for the customer, and if it does exist, click the case number in the results table.

2. If the case does not exist, create one for the customer.

3. Click **Temporary Allow** on the menu bar.

4. In the **Allow** list, select the desired temporary allow.

   - **Single Login**

   - **Two Hours**

   - **Select End Date**

     If you select **Select End Date**, click the calendar icon and click the end date you want.

   - **Cancel**

     If you want to terminate an active allow for a customer, select **Cancel** to remove it

5. In the **Canned Notes** list, select the type of note you want.

6. Edit the note to add information about the action you are taking.

   For example, you can add notes about the actions taken and that the customer is on his trip for three months and should receive an exception for that time.

7. Click **Submit**.

**Temporary Allow Example**

Rita is blocked user and cannot login to bank account and is on vacation in Mexico. She needs to login in next 2 hours to transfer some money to her account since her mortgage payment is coming up. She calls Carl (CSR) and requests to let her login for next 2 hours only.

Carl performs these steps:

1. Carl searches for Rita's logins and asks her when she logged in last time and from where.

2. He crosschecks that information with session data that he sees.

3. Carl creates a case for Rita.

4. He opens that case and creates a temporary allow for Rita for 2 hours.

## 4.12 Performing Case Actions

You can perform the following case actions:

- Adding Notes to Cases

- Changing Severity Level of a Case

- Changing Status of a Case

- Extending Expiration

- Escalating a Case

- Escalating a CSR Case to an Agent Case

- Bulk-Editing CSR Cases

### 4.12.1 Adding Notes to Cases

Each time you take an action in a case you should enter a note describing why you are taking the action. The notes are saved to the case log.

To add notes to cases:

1. From the **Cases Search** page, search for the case from the **Cases Search** page.

   For information, see Section 4.4.1, "Searching for Cases."

2. Click the case number of the case you want.

   The **Case Details** page appears (Figure 4–2).

3. Click **Add Notes** on the menu bar.

   The **Add Notes** screen appears.

*Figure 4–10   Add Notes*



4. Select or enter a note.

5. Click **Submit**.

   If you click **Cancel**, the **Add Notes** screen is dismissed.

   If you click **Submit**, the notes are saved to the case log.

### 4.12.2 Changing Severity Level of a Case

When a case is created it is assigned a severity level to indicate its importance and allow administrators to filter cases. The severity level is shown on the **Case Details** page.

1. Search for the case from the **Cases Search** page.

   For information, see Section 4.4.1, "Searching for Cases."

2. Click the case number of the case you want.

   The **Case Details** page appears (Figure 4–2).

3. On the menu bar, click **More Actions**, and then click **Change Severity**.

   The **Change Severity** screen appears.

4. In the **Severity List**, click the severity level you want.

   The available severity levels are **High**, **Medium**, and **Low**. 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 deescalate the severity level of a case when necessary.

5. In the **Canned Notes** list, select the type of note you want.

6. Edit the note to add information about the action you are taking.

7. Click **Submit**.

### 4.12.3 Changing Status of a Case

Status refers to the current state of a case. The status of a case can be new, pending, or closed. OAAM Admin automatically assigns the status of **New** to each case when it is created. You must change the status to **Pending** after the case is escalated.

1. Search for the case from the **Cases Search** page.

   For information, see Section 4.4.1, "Searching for Cases."

2. Click the case number of the case you want.

   The **Case Details** page appears (Figure 4–2).

3. In the menu bar, click **More Actions**, and then click **Change Status**.

   The **Change Status** screen appears.

4. In the **Status** list, click the status you want.

   You can select **New**, **Pending**, or **Closed**.

*Table 4–5    Case Status*

| Status | Definition |
| --- | --- |
| New | The status of a case when it is created. |
| Pending | The status of a case that is not yet resolved. |
| Closed | The status of a case when the issue is resolved. |
| Escalated | The status of a case that has been escalated. |

5. If status is changed to **New** or **Pending**, extend the expiration date.

6. If status is changed to **Closed**, enter the disposition.

7. Enter a note describing the issue.

   You can select from existing notes or enter a new note.

8. Click **Submit**.

   A confirmation dialog is displayed.

9. Click **OK**.

#### 4.12.3.1 Changing Case Status to Pending

Pending is the status of a case that is not yet resolved. To change the case status to pending.

1. In the Navigation tree, double-click **Cases**.

The **Cases Search** page is displayed.

2. For **Case Status**, select **New**.

   For information, see Section 4.4.1, "Searching for Cases."

3. Click the case number of the case you want.

   The **Case Details** page is displayed (Figure 4–2).

4. In the menu bar, click **More Actions**, and then click **Change Status**.

   The **Change Status** screen appears.

5. For **Status**, select **Pending**.

6. Enter a note describing the issue.

   Select a description from the **Canned Notes** list or enter a new note.

7. Click **Submit**.

   A confirmation dialog is displayed.

8. Click **OK**.

### 4.12.3.2  Closing a Case

Closed is the status of a case when the issue is resolved. To close a case:

1. In the Navigation tree, double-click **Cases**.

   The **Cases Search** page is displayed.

2. For case status, select **New** or **Pending**.

   For information, see Section 4.4.1, "Searching for Cases."

3. Click the case number of the case you want.

   The **Case Details** page appears (Figure 4–2).

4. Click **More Actions** on the menu bar, and select **Change Status**.

   The **Change Status** screen appears.

5. For **Status**, select **Closed**.

6. Select a disposition from the **Disposition** list.

7. Enter a note describing the issue.

   Select a description from the **Canned Notes** list or enter a new note.

8. Click **Submit**.

   A confirmation dialog is displayed.

9. Click **OK**.

### 4.12.3.3  Authenticating Closed Cases

To authenticate a closed case:

1. In the Navigation tree, double-click **Cases**.

   The **Cases Search** page is displayed.

2. Search cases by case status **Closed**.

   For information, see Section 4.4.1, "Searching for Cases."

3. Click the case number of the case you want.

   The **Case Details** page appears (Figure 4–2).

4. Click **More Actions** on the menu bar, and select **Change Status**.

   The **Change Status** screen appears.

5. In the **Status** list, select **New** or **Pending**.

6. Extend the expiration date.

7. Enter a note describing the issue.

   You can select from existing notes or enter a new note.

8. Click **Submit**.

## 4.12.4 Extending Expiration

To extend expiration:

1. In the Navigation tree, double-click **Cases**. The **Cases Search** page is displayed.

2. Search for the case from the **Cases Search** page.

   For information, see Section 4.4.1, "Searching for Cases."

3. Click the case number of the case you want.

   The **Case Details** page appears (Figure 4–2).

4. Click **More Actions** on the menu bar, and select **Extend Expiration Date**.

5. In the **Extension** list, select the length of time you want the expiration to be extended to.

6. In the **Canned Notes** list, click the note you want you want to add.

7. Click **Submit**.

## 4.12.5 Escalating a Case

To escalate a case:

1. In the Navigation tree, double-click **Cases**. The **Cases Search** page is displayed.

2. Search for the case from the **Cases Search** page.

   For information, see Section 4.4.1, "Searching for Cases."

3. Click the case number of the case you want.

   The **Case Details** page appears (Figure 4–2).

4. On the toolbar, click **More Actions** and then select **Escalation**.

   The **Escalation** screen is displayed.

5. In the **Type** list, select the type of case you want the case to be escalated to.

6. Provide notes for the case.

   You can provide notes by selecting notes from the **Canned Notes** list or entering notes in the **Notes** box, or both.

   - From the **Canned Notes** list, select a note to describe the reason for the escalation.

   - In the **Notes** box, enter notes if further details are needed.

7. Click **Submit**.

## 4.12.6 Escalating a CSR Case to an Agent Case

To escalate a case so that Investigators can review it:

1. In the Navigation tree, double-click **Cases**. The **Cases Search** page is displayed.

2. Search for the case from the **Cases Search** page.

   For information, see Section 4.4.1, "Searching for Cases."

3. Click the case number of the case you want the Investigator to review.

   The **Case Details** page appears (Figure 4–2).

4. On the toolbar, click **More Actions** and then select **Escalation**.

   The **Escalation** screen is displayed.

5. In the **Type** list, select **Escalate to Agent Case**.

6. Provide notes for the case.

   Notes are required.

   You can provide notes by selecting notes from the **Canned Notes** list or entering notes in the **Notes** box, or both.

   - From the **Canned Notes** list, select a note to describe the reason for the escalation.

   - In the **Notes** box, enter notes if further details are needed.

7. Click **Submit**.

   The case is escalated to an Agent case and as a CSR, you no longer have permissions to see the case.

## 4.12.7 Bulk-Editing CSR Cases

The **Cases Search** page enables you to change the severity, and status, and extend the expiration date for multiple cases at once. For example, you can close all cases more than a year old.

When the status of the case is set to **New** or **Pending**, you are able to extend the expiration. The option of changing the disposition is not available. When the status of the case is set to **Closed**, you can change the **Disposition**. The option of changing the expiration is not available.

To change the case settings for multiple cases at once:

1. In the Navigation tree, double-click **Cases**. The **Cases Search** page is displayed.

2. Select the cases you want.

   For example, you can search cases by type, expiration, and date.

   For information, see Section 4.4.1, "Searching for Cases."

3. Click **Bulk Edit Selected**.

   The **Bulk Edit** screen is displayed.

*Figure 4–11 Bulk Edit*
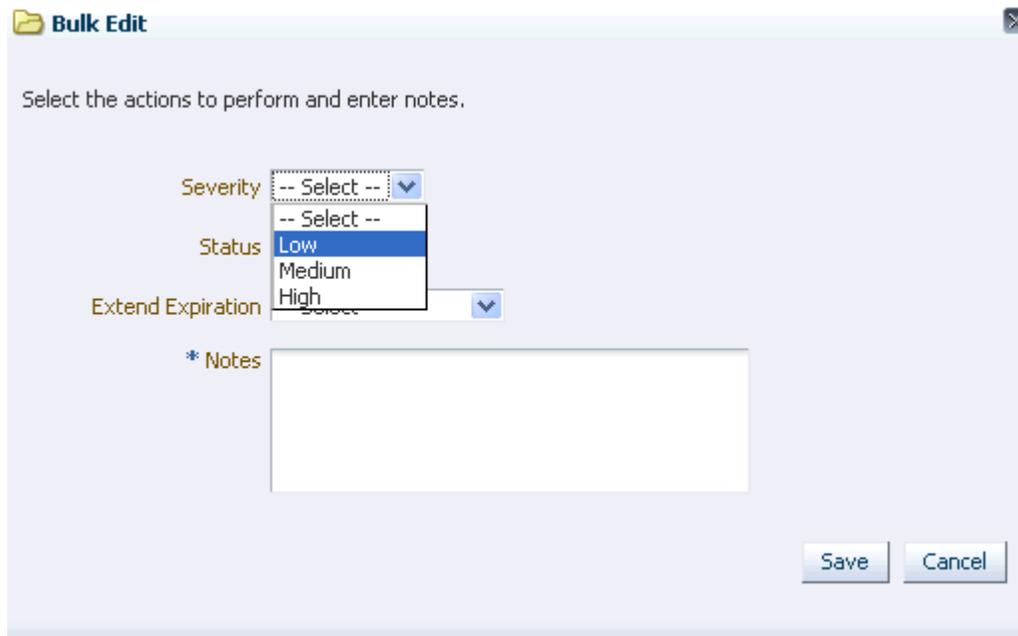


4. Change the case settings you want and add notes.

5. Click **OK** to perform the bulk edit.

   A confirmation dialog appears with a message that the bulk editing operation was performed successfully.

6. Click **OK** to dismiss the dialog.

**Bulk Editing Example**

Jackie needs to cleanup case back log.

1. She goes ahead and searches for all the expired cases and closes them all.

2. She also goes to all overdue cases and updates the status to pending again.

## 4.13 Configuring Expiry Behavior for CSR Cases

The default setting is for CSR cases to expire after 24 hours. After a CSR case expires, a CSR cannot access them. CSR Managers have to extend the expiration time so that the CSR can access them.

The properties for setting and disabling expiry behavior are as follows:

To set expiry behavior for CSR cases (default setting), modify the following properties:

```
customercare.case.expirybehavior.enum.csrcase.behavior = expiry
customercare.case.expirybehavior.enum.csrcase.label = Expired
customercare.case.expirybehavior.enum.csrcase.durationInHrs = 24
customercare.case.expirybehavior.enum.csrcase.resetonaccess = false
```

To disable the expiry behavior for CSR cases, modify the following property:

```
customercare.case.expirybehavior.enum.csrcase.behavior = none
```

> **Note:** You do not need to change the other parameters.

For information on modifying properties, see Chapter 28, "Using the Properties Editor."

## 4.14 Reporting

For information on how CSRs use the reporting functionality of Oracle Adaptive Access Manager, see Chapter 25, "Configuring BI Publisher Reports."

## 4.15 Multitenancy

In multitenant deployment the CSR's access is limited to only those organizations to which they are supposed to be servicing. CSRs can work with the cases that are associated to the users of only those organizations that they service. Agents do not see and work on cases for the users of other groups for which they do not have access.

### 4.15.1 Enabling Multitenancy

To turn on the access control in OAAM Admin for multitenant deployments, you must set the bharosa.multitenant.boolean property to true. By default, the value is set to false.

### 4.15.2 Changing Permissions

The Security Administrators of the OAAM application can set up access control for the CSRs. CSRs cannot change their own access permissions. Only system administrators are able to change access permissions.

### 4.15.3 Access to Cases

CSRs can access cases for the users of groups that they have access permissions to. They cannot access cases for the users of groups that they do not have access to Agent cases cannot be accessed by CSRs.

If multitenancy is disabled, the CSR Manager, Investigator and Investigation Manager have access to details screens (links do not appear). If multitenancy is enabled, the CSR Manager, Investigator and Investigation Manager do not have access to details screens (links do not appear). The CSR never has access to details screens.

From the Session Details page the Investigator cannot get to the Detail screens if multitenancy is on (links are disabled). Multitenant access control only applies for CSRs and Investigators. Security Administrators and System Administrators have full access to cases.

### 4.15.4 Searching Sessions

CSRs and Investigators can only view sessions from organizations they have access to. If Investigators have access to multiple organizations, they should be able to apply the search filters to view sessions from specific organizations. If you have access to an organization, you can search their sessions by Organization ID, Session ID, Alert Level, User Name, Device ID, IP Address, Authentication Status, and Login Time.

### 4.15.5 Examples of Multitenancy in OAAM

The following examples illustrate the user seeing restricted amounts of data on the customer care screens based on permissions.

**Table 4–6    CSR Access**

| Organization | Application Users | Admin Users |
|---|---|---|
| Default | | |
| | ■ demouser1 | ■ democsr1 |
| | ■ demouser2 | ■ democsr2 |
| | ■ demouser3 | ■ democsr3 |
| Org2 | | |
| | ■ org2user1 | ■ org2csr1 |
| | ■ org2user2 | ■ org2csr2 |
| | ■ org2user3 | |
| Both organizations | | |
| | | ■ supercsr1 |
| | | ■ supercsr2 |
| No organization | | democsrm1 |

In the examples, there are two organizations: default and Org2.

### 4.15.5.1  CSR Creates a Case

CSR named "democsr1" has permission for group "Default."

1.  The CSR "democsr1" logs in to the system.

2.  He selects the Organization ID, "Default."

    He can choose "Default" because he has access only to "Default."

3.  He enters "demouser1" in the User Name field and other attributes.

    A case for "demouser1" is created.

    The Case Details page appears.

    ■   The Case Status is "Pending."

    ■   The Created By field shows "democsr1."

    ■   The Current Owner field shows "democsr1."

4.  He searches for the case in the Log tab, and sees the "Create Case" action with ARM ID "democsr1."

5.  A session corresponding to the case exists.

6.  The CSR, "democsr1" adds notes to the case. (CSRs can add notes to a case.)

7.  He goes back to the Logs tabs, and the action for the case is now "Add Notes."

### 4.15.5.2  CSR is unable to Create Case Successfully for Organization and Login Combination

CSR named "org2csr1" has permission for group "Org2."

1.  The CSR logs in to the system.

2.  The only Organization ID he can choose from is "Org2" because he has access only to "Org2."

3.  He tries to create a case for "demouser1."

- He selects the Organization ID, "Org2"

- He enters "demouser1" as the user name.

  demouser1 is a member of "Default."

4. An error is displayed:

"Invalid application Org2 and login demouser1 combination.

### 4.15.5.3 CSR is able to Create Case Successfully for Organization and Login Combination

CSR named "org2csr1" has permission for group "Org2."

1. The CSR logs in to the system.

2. The only Organization ID he can choose from is "Org2" because he has access only to "Org2."

3. He tries to create a case for "demouser1."

   - He selects the Organization ID, "Org2"

   - He enters "org2user1" as the user name.

     org2user1 is a member of "Org2."

4. The case is created successfully.

### 4.15.5.4 CSR Has Access to More Than One Organization ID Is Unable to Create Case

CSR named "supercsr1" has permission for groups "Org2" and Default.

1. The CSR logs in to the system.

2. Both Organization IDs "Org2" and "Default" are available from the dropdown.

3. He tries to create a case for "org2user1."

   - He selects the Organization ID, "Default"

   - He enters "org2user1" as the user name.

     org2user1 is a member of "Org2."

4. An error appears with information that he cannot choose Default as the Organization ID and create a case for a Org2 user.

### 4.15.5.5 CSR Has Access to More Than One Organization ID is able to Create Case Successfully

CSR named "supercsr1" has permission for groups "Org2" and Default.

1. The CSR logs in to the system.

2. Both Organization IDs "Org2" and "Default" are available from the dropdown.

3. He tries to create a case for "org2user1."

   - He selects the Organization ID, "Org2"

   - He enters "org2user1" as the user name.

     org2user1 is a member of "Org2."

4. The case is created successfully.

### 4.15.5.6 CSR Who Cannot Access Any Organization Tries to Create Case

CSR named "democsrm1" cannot access any organization.

1. The CSR logs in to the system.

2. He tries to create a new case, but he cannot select any Organization ID because he does not have access to any organization. He cannot create a new case with the necessary attribute.

3. When he tries a search, there are no results.

### 4.15.5.7 CSR Acts On Case

CSR named "org2csr1" has permission for group "Org2."

1. The CSR logs in to the system.

2. He performs a search.

   a. The Organization ID dropdown presents all the Organization IDs which he has access to.

   b. CSR selects the desired Organization IDs.

   c. CSR provides the data required for his search.

3. The results are Org2 users only.

   The CSR gets back the result which has only those cases whose users belong to group that he has access to.

### 4.15.5.8 CSR Views Case Details

CSR named "org2csr1" has permission for group "Org2."

1. The CSR finishes scenario "CSR Acts On Case".

2. From the search screen, CSR clicks one of the Case IDs.

   a. CSR is able to see the details of the case.

   b. In the bottom half of the tab he sees action logs for the case.

### 4.15.5.9 CSR Searches Sessions

CSR named "org2csr1" has permission for group "Org2."

1. The CSR finishes scenario "CSR Views Case Details".

2. From the case details page, CSR clicks Search Sessions.

   CSR is able to see only the Organization IDs that he has access to in the search query.

3. CSR selects the Organization IDs he is interested in, fills in the other data for the filters, and performs the search.

   Only the results of the sessions of the users of the groups that he has access to is shown.

### 4.15.5.10 Agent Creates a Case

For information, refer to Section 5.5.5, "Creating an Agent Case Manually."

### 4.15.5.11 CSR Searches Cases

For information, refer to Section 5.4, "Searching for Cases."

## 4.16 Use Cases

The following sections provide scenarios of how Oracle Adaptive Access Manager's investigation tools are used.

### 4.16.1 Use Case: Customer Session Search and Case Creation

Carl is Dollar Bank CSR.

Tim calls Carl because he unable to login because he is blocked.

1. Carl searches for blocked sessions by user to determine if any belong to Tim and creates a case when he finds none for Tim.

   a. Carl must search sessions for users with blocked logins.

   b. Carl must search first the session for "Tim" and see his logins history for last one month.

   c. He then must search for cases that might be there for Tim.

      Carl finds no cases for Tim.

2. Carl creates a case by choosing out-of-the-box texts for blocked login.

   Some days pass and Tim calls again to find out about the case.

3. Carl finds the case and sees that it has expired.

4. Carl escalates the case. After escalation he no longer sees the case in the search.

Jackie is CSR Manager.

1. She logs in and searches for escalated cases.

2. She finds Tim's case and views it.

3. She looks at the action logs of the case and figures who created and acted on it.

4. She adds notes to the case saying she is working on it.

### 4.16.2 Use Case: Reset Challenge Questions

You are Jerry, a customer service representative at Acme Corp. You answer phones at the call center and assist users with issues they may be experiencing. You received a call from Henry, a user who has forgotten the answers to his challenge questions. You must verify his personal information before you can reset his answers.

Directions: Part A: Authenticate Henry in another system by verifying personal information such as home address and last four digits of his Social Security Number. His User ID is xxxx.

Directions: Part B: Then, open a new CSR case for Henry and reset his challenge questions.

Directions: Part C: Now, close the case with a resolved disposition and notes.

1. Log in to OAAM Admin as a Customer Service Representative.

2. In the Navigation tree, double-click **Cases**. The **Cases Search** page is displayed.

3. In another system enter Henry's User ID and verify his home address and last four digits of his Social Security Number.

4. Search open cases by user.

Search for Henry's open cases by entering xxxx into the **User ID** field and selecting **New**, **Pending**, and **Escalated** for his case status.

New, pending, and escalated cases do not exist for Henry; therefore, you must create a new case.

5. Create a new case.

   a. In the **Cases Search** page, click the **New Case** button.

      The **Create Case** screen is displayed.

   b. Enter the Henry's user name, xxxx, in the **User ID** field and select the **Organization ID** (group Henry belongs to).

   c. For severity level, select **Low** from the **Severity Level** list

      The available severity levels are **High**, **Medium**, and **Low**.

   d. Select **Forgot question answers** from the **Description** list.

   e. Click **Create**.

      The **Create** button is disabled until all the fields are entered.

      If invalid parameters were entered, an error message is displayed and the new case is not created.

      If you click **Create**, the new case is created.

      A confirmation message appears.

   f. Click **OK** to dismiss the confirmation message.

6. Reset Henry's questions.

   a. To reset Henry's questions, in the **Case Details** page, select **More Actions** and then select **Challenge Questions**.

      Authenticator uses questions as additional credentials to help prevent fraud. From the **Challenge Questions** screen, you can perform questions-related actions for the customer when necessary.

   b. In the **Item** list, select **Reset Questions** as the question-related action to perform.

   c. In the **Canned Notes** list, select **Forgot Question/Answers**.

   d. Click **Submit** to reset Henry's questions.

      When you reset a customer's challenge questions, OAAM Admin deletes the existing questions and answers and generates a new question set for customers to register from.

      A confirmation message appears.

   e. Click **OK** to dismiss the dialog.

7. Add notes on the case.

   Each time you take an action in a case you should enter a note describing why you are taking the action. The notes are saved to the case log.

   a. Click **Add Notes** on the menu bar to add notes on the case.

   b. Enter a note that Henry's challenge questions were reset.

   c. Click **Submit**.

      If you click **Submit**, the notes are saved to the case log.

A confirmation message appears.

d. Click **OK**.

8. Inform Henry that he will go through challenge questions registration (select new questions and answers from his question set) the next time he logs in.

9. Close the case with a disposition.

a. To close the case, in the **Case Details** page, click **More Actions** and select **Change Status**.

Case status refers to the current state of a case.

b. In the **Status** list, click **Closed**.

**Closed** is the status of a case when the issue is resolved.

c. For the disposition select **Issue Resolved**.

d. Select **Issue Resolved** from the **Notes** list as the note describing the issue.

You can select from existing notes or enter a new note.

e. Click **Submit**.

A confirmation message appears.

f. Click **OK** to dismiss the dialog.

### 4.16.3 Use Case: Reset Image and Phrase

You answer a call from Nancy, a user who does not like the virtual device personalization she registered. She would like you to change it for her. You explain that Nancy can do this herself on the **User Preferences** page of the Authenticator, but she insists that you reset her image and phrase.

Directions: Part A: Open a new CSR case for Nancy and reset her image and phrase. You tell her that her virtual authentication device will show a new image and phrase the next time she logs in.

Directions: Part B: Then, close the case with a resolved disposition and enter some pertinent notes.

1. Log in to OAAM Admin as a Customer Service Representative.

2. In the Navigation tree, double-click **Cases**. The **Cases Search** page is displayed.

3. Search open cases by user.

Perform a search by case number or by Nancy's **User ID** and a **Case Status** of **Open**, **Pending**, or **Escalated** to find out whether a case already exists.

Since an open case to reset her personalization does not exist, you create a new case.

4. Open a new case.

a. Click **New Case** to create a new case.

The **Create** button is disabled until all the fields are entered. No fields can be left blank.

b. Enter the required details.

c. Click **Create**.

If invalid parameters were entered, an error message is displayed and the new case is not created.

If you click **Create**, a new case is created and a confirmation dialog is displayed with the Case ID number.

d. Click **OK** in the **Create Case** confirmation dialog.

The **Case Details** page for the newly created case is displayed.

5. Reset the user's image and phrase.

a. In the menu bar of the **Case Details** page, select **Customer Resets**. The **Customer Resets** screen appears.

b. In the **User Item** list, select **Image and Phrase**.

c. In the **Canned Notes** list, select the type of note you want to add.

d. In the **Description** field, modify the description to suit your needs.

e. Click **Submit**. A confirmation dialog is displayed with the message that the customer has been assigned a new image and phrase.

f. In the confirmation dialog, click **OK**.

When you reset a customer's image and phrase, OAAM Admin generates a new image and phrase and assigns them to the customer.

6. Tell Nancy that her virtual authentication device will show a new image and phrase the next time she logs in.

7. Close the case with a disposition.

a. In the menu bar, click **More Actions**, and then click **Change Status**.

The **Change Status** screen appears.

b. In the **Status** list, click **Closed**.

c. For the disposition, select **Issue Resolved**.

d. Enter a note describing the issue.

You can select from existing notes or enter a new note.

e. Click **Submit**. A confirmation dialog is displayed with the message that the case status was successfully saved.

f. Click **OK** to dismiss the dialog.

## 4.16.4 Use Case: Bulk Edit CSR Cases

You are Mike, a customer service manager at Acme Corp. The company policy for CSR cases is that cases should be closed as soon as the user issue is resolved. After a month you close out any CSR cases that have been left open by mistake. Directions: Today is the end of the month, so you are going to bulk-close any cases older than 24 hours and newer than a month ago.

To bulk edit CSR cases:

1. Log in to OAAM Admin as a Customer Service Representative Manager.

2. In the Navigation tree, double-click **Cases**.

The **Cases Search** page is displayed.

3. Search the pending CSR cases created between a month ago and yesterday.

    **a.** In the **Case Status** field, select **Pending**.

    **b.** For **Created Date**, enter the date and time for the last day of the previous month.

    **c.** For **End Date**, enter the date and time 24 hours ago.

    **d.** Click **Search**.

**4.** Select all cases and close them with a disposition and notes.

    **a.** Select all cases listed in the **Search Results** table.

    **b.** Click the **Bulk Edit** icon on the **Search Results** toolbar.

    The **Bulk Edit** screen appears.

    **c.** In the **Status** list, click **Closed**.

    **d.** For the disposition, select **Issue Resolved**.

    **e.** Enter a note that says that the case was left open by mistake.

    **f.** Click **OK**. A confirmation dialog is displayed with the message that the bulk editing operation was performed successfully.

    **g.** Click **OK** to dismiss the dialog.

## 4.16.5 Use Case: CSR Manager Bulk Case Edit

Carl is Dollar Bank CSR manager. He comes into work each morning and searches through the CSR cases to check on status and clean up if needed. First he runs a search for CSR cases that are expired. There are four cases with the **Expired** status, so Carl looks at the creation dates for each. All are more than two days old. One of them has a **High** severity and the last action was a **Temp Allow**. The other three were **Low** severity cases with **Phone Challenge** as the last action. He selects these three and closes them with a disposition of **expired and resolved**. Carl opens the high severity case to look at the log. He sees that the temporary allow is active for another week so he leaves the case in the expired status as a marker.

**1.** Log in to OAAM Admin.

**2.** In the Navigation tree, double-click **Cases**. The **Cases Search** page is displayed.

**3.** In the **Expired** field, select **Show Only Expired**.

**4.** In the **Case Type** field, select **CSR**.

**5.** Click **Search**

There are four cases with the **Expired** status.

**6.** View **Created Date** column for the four cases in the **Search Results** table.

- All are more than two days old. (View **Created Date**)

- One of them has a **High** severity and the last action was a **temp allow**. (View **Case Severity** and **Last Action Type** columns.

**7.** Select the three cases and click **Bulk Edit**.

**8.** In the **Status** field, select **Closed**.

**9.** In **Deposition** field, select **Issue Resolved**.

**10.** In **Notes**, enter `expired and resolved`.

**11.** Click the **Case ID** for the **High** severity case.

**12.** In the **Case Details** page, view the log for log code and notes.

### 4.16.6 Use Case: CSR - Ask Questions

User "customer" is a registered user. He has not been challenged for the past 30 days and when he had to answer a challenge question, he completely forgot the answer to this question. He is sure he remembers the answers to his other questions. User answers the question incorrectly all 3 times. Before he could try it out, he is blocked. He calls customer support, and the CSR creates a case and asks challenge questions. She enters the user's answers until he answers correctly or is locked out. He answers the question correctly. He is unlocked and is able to login successfully. The CSR informs the user he must register new questions online next time he logs in. The CSR closes the case.

## 4.17 Best Practices and Recommendations

This section provides best practices and recommendations:

- A Fraud Investigator looks into suspicious situations either escalated from customer service or directly from OAAM Admin alerts.

- A Fraud Investigation Manager determines which cases must be given attention by his team.

- If a customer suspects fraud, then the severity level assigned is **High**. For example, if the customer wants a different image, then the severity level assigned is **Low**. Severity levels of a case can be escalated or deescalated when necessary. Anyone can change the severity of cases.

# 5

# Investigation Using Agent Cases

Oracle Adaptive Access Manager allows the creation of Agent cases to make forensic investigations quicker, easier and more successful. Investigators can link relevant sessions that may be connected to fraud cases to locate relationships between data that is linked, sessions in which suspicious activity occurred, or sessions in which alerts were generated. Investigators can link suspicious sessions. They can also unlink sessions that they think are no longer suspicious.

This chapter provides information to Investigators for using the new Agent cases. It contains the following sections:

- Introduction and Concepts
- Fraud Investigation Role Permission
- Opening the Case Search Page
- Searching for Cases
- Viewing, Editing, and Creating Cases
- Editing Agent Cases
- Linking and Unlinking Suspected Sessions to a Case
- Agent Case Feedback
- Configuring Agent Case Access
- Configuring Expiry/Overdue Behavior for Agent Cases
- Agent Use Cases
- Best Practices and Recommendations

## 5.1 Introduction and Concepts

This section provides an introduction to Investigators and a high-level view of how they might use the Oracle Adaptive Access Manager Agent cases to investigate fraudulent activity.

### 5.1.1 Agent Cases

An Agent case is a tool used for investigation. It can be created manually or automatically.

- A CSR creates an Agent case when he escalates a case because further investigation from an Investigator is needed. Refer to Section 5.1.2.3, "Escalated Cases."

- A fraud investigator creates an Agent case when a suspicious activity or fraud scenario is detected and needs investigation.

- A configurable action creates an Agent case automatically as a supplementary action that is triggered based on a result action and/or risk score after a checkpoint execution.

**Agent cases** are not created for specific users. They are created for specific scenarios. Events can be configured to create a case automatically. Agent type cases are used by fraud investigators to do the following:

- Collect investigation findings for audit including which investigators have worked on a case

- Manage the lifecycle of an investigation including severity, status, ownership changes, time to resolution, dropped/lost cases and resolution

- When closed findings are fed back into the risk engine to improve accuracy of future evaluations automatically

- Export findings to Excel for external records or processes

A fraud investigator can quickly view the data involved in an incident and quickly locate related situations by easily harnessing the complex data relationships captured by OAAM. Search and detail pages provide fraud investigators the ability to:

- Drill into individual sessions to see the exact chain of events that led to an alert

- View and search for complex relationships between different data types

- White/black list entities "on the fly" without leaving the investigation flow

- Link session data to a case to further narrow the investigation

## 5.1.2 Case Status

**Case Status** is the current state of a case. Status values used for the case are **New**, **Pending**, **Escalated**, or **Closed**.

*Table 5–1   Case Status*

| Status | Definition |
| --- | --- |
| New | The status of a case when it is created. |
| Pending | The status of a case that is not yet resolved. |
| Closed | The status of a case when the issue is resolved. |
| Escalated | The status of a case when a CSR escalates a case. |

### 5.1.2.1 New and Pending Cases

Cases are "New" when they are created regardless of the method (manual/configurable action). When a new case is accessed for the first time, the status automatically changes to "Pending." For example, if an Agent case is created by a configurable action, it contains the session data for which it was created and it has a "New" status. If an investigator searches for all Agent type cases with a "New" status, and he opens the case details page for one of the new cases, the case status automatically changes to "Pending". This allows Investigators to know if someone is already working on a case.

### 5.1.2.2 Closed Cases

Closed is the status of a case when the issue is resolved.

### 5.1.2.3 Escalated Cases

If a CSR case is escalated to an Agent case, the status changes to "Escalated" in the process. The first time an investigator accesses the case, the status changes to "Pending" automatically. The CSR escalates a case when he cannot resolve a case and needs further investigation by an investigator or when he determines there is suspicious activity associated with the specific user and he wants further investigation by an investigator. Once escalated the case is treated as an Agent case, which is no longer visible to the CSR. However, any agent can work on the escalated case.

## 5.2 Fraud Investigation Role Permission

**Fraud Investigator** and **Fraud Investigation Manager** are out-of-the-box roles provided by Oracle Adaptive Access Manager. A **Fraud Investigator** investigates a specific fraud scenario or suspicious pattern. In order to work on the scenario or pattern, he creates an Agent case. A **Fraud Investigation Manager** has access to actions that the Fraud Investigator does not have. They can reopen closed cases and bulk edit cases. To act upon the fraudulent sessions, they create Agent cases, and then link the fraudulent sessions to the case. Based on the type of fraud, they perform further case actions.

The out-of-the-box permissions associated with fraud investigation are summarized in Table 5–2. Additional actions are listed in Appendix A, "Access Roles."

*Table 5–2    Fraud Investigation Role Permissions*

| Action | Investigator Permissions | Investigation Manager Permissions |
|---|---|---|
| Actions | All functions of Investigator role | All functions of Investigator role and some special privileges |
| Search Cases | ■ Search for CSR, Escalated and Agent cases<br>■ Search for open and closed cases | ■ Search for CSR, Escalated and Agent cases<br>■ Search for open and closed cases. |
| New Case | Only Agent cases | Only Agent cases |
| View Case Details | ■ View Escalated Case<br>■ View closed case details | ■ View Escalated Case<br>■ View closed case details |
| Edit Case | ■ Add notes to CSR and Escalated Cases<br>■ Change status and severity<br>■ Cannot bulk edit cases<br>■ Escalate cases | ■ Add notes to CSR and Escalated Cases<br>■ Reopen closed cases<br>■ Change status and severity<br>■ Bulk edit cases<br>■ Escalate cases |
| Search session | Search sessions | Search sessions |
| Link sessions | Link sessions | Link sessions |
| Unlink sessions | Unlink sessions | Unlink sessions |
| View linked sessions | View linked sessions | View linked sessions |

## 5.3 Opening the Case Search Page

To perform the operations listed earlier, log in as an Investigator. Open to the **Cases Search** page by double-clicking **Cases** in the Navigation tree.

Alternatively, you can open the **Cases Search** page by:

- Right-clicking **Cases** in the Navigation tree and selecting **List Cases** from the context menu.

- Selecting **Cases** in the Navigation tree and then choosing **List Cases** from the **Actions** menu.

- Clicking the **List Cases** button in the Navigation tree toolbar.

The **Cases Search** page contains the search tools to help you find cases that you are interested in. The **Search Results** table displays a list of cases that meet the criteria you specified. If you upgraded your environment, agent cases from previous releases are also visible. There is a link on the case number. To view the case details, click the link. All search tables and dialog boxes should have asterisks for the required fields.

## 5.4 Searching for Cases

The **Cases Search** page contains the search tools to help you find cases that you are interested in.

1. From the **Cases Search** page, specify criteria in the Search Filter.

*Table 5–3    Search Filters*

| Filter | Description |
| --- | --- |
| Organization ID | To locate cases for an organization, select the Organization ID. CSRs can choose one from a list of Organization IDs of organizations which they have access to. |
| User Name | The User Name field is blank for Agent cases. |
| User ID | The UserID field is blank for Agent cases. |
| Case ID | To locate a specific case, enter the Case ID. |
| Description | To locate a case by a keyword that is in the description, enter the word you want. Search by description displays all cases with any matching words in the description field. |
| Case Type | To filter cases by case type, select Agent. |
| Severity Level | To filter cases by severity level, select Low, High, or Medium. |
| Case Status | To filter cases by case status, select New, Pending, Closed, Escalated. |
| Expired | To filer the list by expired, select the option you want. The options available are: <br>- Hide Expired <br>- Show Only Expired |
| Created Date | To locates cases created within a given create date range, enter the start and end dates you want for the range. |

*Table 5–3   (Cont.) Search Filters*

| Filter | Description |
| --- | --- |
| Disposition | To filter cases by dispositions, you can select: |
| | ■  Confirmed Fraud |
| | ■  Duplicate |
| | ■  False Negative |
| | ■  False Positive |
| | ■  Issue Pending |
| | ■  Issue Resolved |
| | ■  Not Fraud |
| | The disposition describes the way in which the issue was resolved in a case. Cases only have dispositions when they are closed. If a case has any status besides closed, the disposition is left blank. |
| Last Action | Search based on the last action that was taken in case. |
| Notes | Search for cases that contain specific keywords in their log. For example, if you search for all Agent type cases that contain the word "chargeback," a case with a note that contains "The device used seems to be related to a number of chargebacks" would return in the list of cases. |
| Created by | Search by user name of the agent who created the case. |
| Current Owner | Search by user name of the agent who is working on this case currently (who performed the last action) |

2.  Click **Search**.

    If multitenancy is enabled, search results display all the cases whose users belong to the organizations that the CSR has access to if they match the search criteria. User less cases are part of the result set if the case owner's Organization ID is on the agent's access permission list and the case matches the search criteria.

### Searching for Overdue Cases

By default Escalated and Agent cases expire after 24 hours and become overdue. The overdue flag is then set. When Investigators access the case, the expiration date is reset. To search for overdue Agent cases, select **Shown Only Expired** as the **Expired** filter. The cases with dates and time in red in the Expiration Column are overdue cases.

*Figure 5–1    Overdue Cases*



## 5.5  Viewing, Editing, and Creating Cases

Procedures to view, edit, and create are listed below.

### 5.5.1  Viewing a List of Cases

From the **Cases Search** page, enter filter criteria and click **Search**. The Search Results table displays the list of cases you filtered for.

### 5.5.2  Viewing a List Cases You are Currently Working On

From the **Cases Search** page, enter your user name in the Current Owner field to locate cases that you are currently working on and click **Search**. The Search Results table displays the list of cases you are currently working on.

### 5.5.3  Viewing Agent Case Details

The Agent Case Details page is opened when you create a case successfully. You can also open the Agent Case Details from the Search results for cases that belong to any user belonging to a group you have access to or cases that are associated with your Organization ID.

> **Note:**   You can only open one case at a time. An error occurs if you try to open more than one case.

Agent and Escalated cases contain the following tabs:

- Summary - Lists the details about the case

- Linked Sessions - Lists the sessions linked to the case

- Logs - Lists the case action logs

The Summary tab shows the case detail and if the case is an Escalated case then it shows the details of the user associated with the case. Agent cases that are user less show a User Details section.

### 5.5.3.1  Summary Tab

The Summary tab shows the case details for Agent cases. If the Agent case is an Escalated case, it also shows the detail of the user associated with the case.

**5.5.3.1.1    Case Details**  The following information is displayed in Case Details.

*Table 5–4    Case Details*

| Details | Description |
| --- | --- |
| Organization ID | The Organization ID of the case. |
| Case Created | The date when the Agent Case was created |
| Case Status | The case status is "Pending" when the Agent Case is created manually and "New" when an Agent Cases is created automatically (with Configurable Action) and changes to "Pending" once the case is accessed. The case status is "Escalated" for Escalated cases and changes to "Pending" when the agent accesses this case. |
| | Case status is changed when accessed by various administrators. |
| Severity Level | The severity level is set by the user who creates the case and used as a marker to communicate to users how severe the case is. Anyone can change the severity of cases |
| Case Type | Agent, CSR or Escalated (Escalated cases cannot be created) |
| Case Number | Unique Case ID |
| Disposition | When a case is closed the disposition describes the way in which the issue was resolved. Cases only have dispositions when they are closed. If a case has any status besides closed, the disposition is blank. |
| Expiration Date | Agent cases and Escalated cases have a default expiration date of 24 hours from the date of creation. If the case has not been accessed before the expiration date, it has the status of Overdue. Each time you access the case, the expiration date of the Agent case or Escalated Case is reset to a new value; by default the date is reset to 24 hours from the date of accessing the case. The length of time before a case expires is configurable. Refer to Section 5.10, "Configuring Expiry/Overdue Behavior for Agent Cases" for details for configuring the expiry behavior. |
| Overdue | If the case has not been accessed before the expiration date, the overdue flag is set to allow managers to see that the cases require attention. For example, if Agent cases are set to expire in 24 hours, then the flag is set to "overdue" if a case has not been accessed in more than 24 hours. When Investigators access the case, the overdue date is not affected. When they perform actions, the overdue is reset. The overdue behavior is configurable. Refer to Section 5.10, "Configuring Expiry/Overdue Behavior for Agent Cases" for details |
| Description | The details for the case. A description is required. |
| Last Case Action | The last action performed in the Escalated or Agent case. There are no user details in Agent cases. |
| Date of Last Case Action | The date when last action occurred. |
| Last Global Case Action | For an Agent case that is not created from an escalated CSR case, the last global case action field is always empty. For an Agent case associated to a user (escalated case), the last global case action is the last case action performed by the user associated with the Agent case. The case action could be performed on any case (CSR/Agent) |

*Table 5–4   (Cont.)  Case Details*

| Details | Description |
| --- | --- |
| Date of Last Global Case Action | The last action performed against the user online. |
| Current Owner | Name of agent who is working on this case currently |
| Created By | This displays the name of the agent who created the case. If the case was created by a configurable action "Created by" displays "dynamic." |

**5.5.3.1.2   User Data**  The following information is displayed in User Data for Escalated cases.

*Table 5–5   User Data*

| Data | Description |
| --- | --- |
| User Name | User for whom case is created |
| User ID | Auto generated? |
| Organization ID | The identifier of the application. (In a multitenant deployment, CSRs 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, the Answered challenge question field show "Challenge Question" or if user is blocked, "Block." |
| Date of Last Online Action | Date when last online action was executed. |
| Temporary Allow Expiration Date | When a temporary allow is enabled. This field shows you when it expires. If temporary allow is 7 days, the expiry date is a week from today. |
| Temporary Allow Active | If temporary allow is active, this field shows "Yes," otherwise the field shows "No." |
| OTP Bypass Active | Similar to temporary allow but OTP challenges are ignored instead of blocks |
| OTP Bypass Expiration Date | Date and time OTP Bypass is no longer be active |
| Completed Registration | If a user completed registration, this field shows "Yes;" otherwise it shows "No." To be registered, a user may need to complete all of the following tasks: personalization (image and phrase), registering KBA questions/answers, and providing email/cell phone contact information. |
| Questions Active | If user completed registration, but questions were reset, and he did not go back to register new ones, this field displays "No." This field shows "Yes" if the user completed registration and questions exist that can be used to challenge him. |
| OTP Delivery method active | User has either email or cell phone registered for the OTP challenge |
| Personalization Active | When an image, a phrase and questions are active for the user, this field displays, "Yes." If anyone of these are reset, this field displays "No." |

### 5.5.3.2  Linked Sessions

The Linked Sessions tab displays all of the sessions that you linked for the case you are investigating. The tab also displays information such as the date at which it was linked and any notes provided at the time of linking. You can link any number of sessions as you think might be connected to an investigation by clicking the Link Sessions icon, which opens a Sessions search page. You can unlink one or more sessions already linked to this case.

**5.5.3.2.1   Logs Tab in the Linked Sessions**  The Logs Tab displays all the actions, date of action, and User IDs that were used for the action and notes.

### 5.5.3.3 Logs

The logs sections to show the logs of action performed on the case. The search filters are as follows:

*Table 5–6    Log Search Filters*

| Filters | Description |
| --- | --- |
| Notes Keyword | Keyword from Canned Notes |
| ARM ID | CSR identifier |
| Action | Last action in the case. For example, yesterday jsmith called customer service claiming to have lost money out of his account. The CSR escalated the case and told jsmith he would be contacted within 24 hours. About 36 hours later, jsmith calls back to see why he has not been contacted. The CSR must view the case escalated yesterday for "jsmith". He searches cases for "jsmith" with an "Escalate" action and ones that are not overdue in the last 48 hours. |
| Created Date | Date case was created. |

## 5.5.4 Creating Agent Cases

Agent cases can be created in one of three ways:

- Manually
- Automatically
- CSR Escalation

## 5.5.5 Creating an Agent Case Manually

A new Agent case is created when a suspicious activity or fraud scenario is detected and needs investigation. Only an Investigator can create an Agent type case directly. No user information is shown or required for the creation of an Agent type case. The only required inputs to create an Agent case are Organization ID, severity, and description.

To create a new user less Agent case:

1.  In the **Cases Search** page, click **New Case**.

    The **Create Case** dialog appears with **Agent** specified as the Case Type because the system already knows from the login that an Investigator is creating this case.

2.  Enter the **Organization ID** you are creating the case for.

    A list of **Organization ID**s for which you have access to is provided. From the list you can select one **Organization ID**. Later, you can create a case for a different Organization ID if you need to.

    > **Note:** You do not have to enter a user name or User ID because the Agent case is a user less one.

3.  Select a severity level from the **Severity Level** list

    The available severity levels are **High**, **Medium**, and **Low**.

4.  Enter a description of the case in the **Description** text box, or select descriptions from the **Description** list, or do both.

The default description type is **Custom Description**. The **Description** text box can contain alphanumeric and special characters, but it should not exceed 4000 characters. You can select a description from the **Description** list, one at a time for any number of times. Each description selected from the list is appended to the previous.

**Description** is a required field. The **Create** button is disabled until a description is entered.

5. Click **Create**.

   The **Create** button is disabled until all the fields are entered. Required fields are marked with a "*" (asterisks). If invalid parameters were entered, an error message is displayed and the new case is not created.

   Click **Cancel** to cancel changes and return to the **Cases Search** page. Click **Create** to create a new case.

   The case is created and the **Case Details** page opens for the new case. For information, refer to Section 5.5.3.1.1, "Case Details." The Case Details page shows "Pending" as the status of the case. The agent is listed in the Created by and Current Owner fields. There are no user details shown in the Case Details because the case is a user less Agent case. The new Agent case does not contain any linked sessions. When you view the logs, **Create Case** is displayed as the Action.

   **Manual Agent Case Creation Example**
   An Agent creates an Agent type case for the 1st Bank Organization ID. He is not given the option to create cases of other types (CSR case). Organization ID is a required field. The new Agent case does not contain any linked sessions. He is not required to enter any user information to create the case since Agent cases are not linked to any single user.

## 5.5.6 Creating an Agent Case Automatically by a Configurable Action

To configure an action so that an Agent case is created automatically:

1. Create a custom rule action called **create_agent_case**.

2. Add a rule with the rule condition you want to a policy for the appropriate checkpoint. Configure it such a way that it triggers and returns the action **create_agent_case** whenever the specified conditions are met. For example, whenever a suspicious activity occurs the create Agent case action is triggered.

3. Create an action instance of the action template **CaseCreationAction** and associate it to the checkpoint.

4. Set the trigger criteria as the action by selecting **create_agent_case** action.

5. Set the parameters of **CaseCreationAction** as follows:

   a. Enter "2" (for Agent type) as value of **Case Type**.

   b. Enter "2" (for Medium) or "3" (for High) for the **Severity**.

   c. Enter a case description. For example, "Failed login."

   d. Enter the userId for "Case Creator UserId" parameter. Make sure that userId has a proper role and access permissions for creating the case. For our example, the Case Creator is Dynamic.

6. Save the action instance.

7. Log in to the application unsuccessfully.

On every unsuccessful log in, you should see an automatic creation of an Agent case by the configurable action. The status of the case is "New." The new Agent case has auto linked sessions based on the action instance parameters. It will contain the session data for which it was created.

There are two logs for the autocreated Agent case: one for creation and one for the link session.

If an Investigator opens the case, the Status of the case changes to "Pending." The Current Owner is the Investigator and the Created by displays the Case Creator UserId. User Details are also shown for this case.

8. Verify that the sessions that correspond to the action instance parameters like checkpoint, score range, execution type are autolinked to the Agent case that is created by the configurable action.

**Agent Case Autocreation Example**

1. A Security Administrator configures an action to create agent cases when specific rules trigger.

   When this case creation action generates a case, the session data in which the rule triggered is added to the case in the form of a linked session.

2. Fraud Investigator opens the OAAM Admin Console and sees only the appropriate user interface views and controls afforded his role.

3. Fraud Investigator searches cases by new status

4. Fraud Investigator opens the case at which time he becomes the current owner and the status of the case changes to pending.

5. He can continue linking session to the case and/or drill in on the data in the linked session using the details screens.

6. When finished, the Investigator closes the case with a disposition and notes.

## 5.5.7 Creating an Agent Case from an Escalation

To escalate a case so that Investigators can review it:

**Escalate CSR to Agent Case Example**

1. CSR Manager escalates CSR case

2. A fraud investigator picks up the escalated type case and reads the notes entered by the CSR and CSR Manager. The status automatically changes from escalated to pending.

3. He searches for the session history of the user.

4. Investigator selects the session from the Ukraine and searches for related sessions and cases. He finds no sessions or cases that seem suspicious

5. He determines that he can safely add the user to the override group for this rule.

6. The investigator then closes the case with a resolved "customer override" disposition.

7. Every three months a security administrator removes all users from the override group.

### 5.5.8 Creating a Case Like Another Agent Case

To create a new case that is similar— or "like"—an existing Agent case:

1.  From the **Cases Search** page, select an Agent case by clicking in the checkbox next to case in the **Search Results** table.

    The **Create Like** button is disabled if you select multiple rows in the **Search Results** table.

2.  Click the **Create Like** button.

    The **Create Case Like** dialog appears with Organization ID, Severity level and description pre-populated from the original case.

3.  Edit any of these fields if you want.

    Do not leave any fields blank.

    The Create button is disabled until the required fields are filled in.

4.  Click **Create**.

    Click **Cancel** to cancel changes and return to the **Cases Search** page.

    Click **Create** to create a new case.

    A new Agent case is created with data from the original case and your changes, and the **Case Details** page opens for the new case. A new Agent case created like an escalated Agent case does not contain any user data. The case status is "Pending."

## 5.6 Editing Agent Cases

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.

### 5.6.1 Adding Notes to Cases

Each time you take an action in a case you should enter a note describing why you are taking the action. The notes are saved to the case log.

To add notes to cases:

1.  In the Case Details page, click **Add Notes**.

    The **Add Notes** dialog appears.

2.  Select a canned note or enter notes in the text box or both.

3.  Click **Submit**.

    The notes are saved to the case log.

4.  Click **OK** to dismiss the confirmation dialog.

### 5.6.2 Changing Severity Level of a Case

When a case is created it is assigned a severity level to indicate its importance and allow administrators to filter cases. The severity level is shown on the **Case Details** page.

1.  In the Case Details page, click **More Actions** and select **Change Severity**.

    The **Change Severity** dialog appears.

2. In the **Severity List**, select the severity level you want.

   The available severity levels are **High**, **Medium**, and **Low**. 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 when necessary.

3. In the **Notes** list, select the type of note you want.

4. If necessary edit the note to add information about the action you are taking.

5. Click **Submit**.

   The case severity is saved to the case log.

6. Click **OK** to dismiss the confirmation dialog.

## 5.6.3 Changing Status of a Case

The status of a case can be changed manually or automatically.

### 5.6.3.1 Changing the Status of a Case Manually

The scenarios show how to change the case status manually.

**5.6.3.1.1 Changing the Status of the Case to New Manually**  To change the status of a case to New manually:

1. In the Case Details page, click **More Actions** and select **Change Status**.

   The **Change Status** dialog appears.

2. In the **Status** list, select **New**.

3. Enter a note describing the issue.

   You can select from existing notes, or enter a new note, or both.

   Existing notes to choose from are the following:

   ■ Manager Review

   ■ Other

4. Click **Submit**.

   A confirmation dialog is displayed.

5. Click **OK**.

**5.6.3.1.2 Changing the Status of the Case to Pending Manually**  To change the status of a case to Pending manually:

1. In the Case Details page, click **More Actions** and select **Change Status**.

   The **Change Status** dialog appears.

2. In the **Status** list, select **Pending**.

3. Enter a note describing the issue.

   You can select from existing notes, or enter a new note, or both.

   Existing notes to choose from are the following:

   ■ Manager Review

   ■ Issue in Progress

■ Other

4. Click **Submit**.

A confirmation dialog is displayed.

5. Click **OK**.

### 5.6.3.2 Configuring Auto Change for Case Status

To enable Auto Change of Case Status set the following parameter:

```
customercare.case.autostatuschange.enum.flowone.enabled=true
```

To disable Auto Change of Case Status set the following parameter:

```
customercare.case.autostatuschange.enum.flowone.enabled=false
```

Configurable actions create cases with a status of "New". When the case is opened, the status is changed to "Pending." For these cases to change from "New" to "Pending" automatically on access, configure the following properties:

```
customercare.case.autostatuschange.enum.flowone=1
customercare.case.autostatuschange.enum.flowone.name=Flow
onecustomercare.case.autostatuschange.enum.flowone.description=Status flow
onecustomercare.case.autostatuschange.enum.flowone.enabled=true
customercare.case.autostatuschange.enum.flowone.from=new
customercare.case.autostatuschange.enum.flowone.to=pending
```

Escalated cases have a Case Status of Escalated. When the case is opened, the status is changed to "Pending". For cases to change from Escalated to Pending automatically on access, configure the following properties:

```
customercare.case.autostatuschange.enum.flowtwo=2
customercare.case.autostatuschange.enum.flowtwo.name=Flow Two
customercare.case.autostatuschange.enum.flowtwo.description=Status flow two
customercare.case.autostatuschange.enum.flowtwo.enabled=true
customercare.case.autostatuschange.enum.flowtwo.from=escalated
customercare.case.autostatuschange.enum.flowtwo.to=pending
customercare.case.autostatuschange.enum.flowtwo.casetype=agent
```

The action log for the auto-change is created with the entry, "Status changed on access by the system."

## 5.6.4 Closing Cases

After an investigator finishes investigating a situation and comes up with a conclusion, he can change the status to close the case and give a disposition.

### 5.6.4.1 Closing a Case Manually

To close a case manually:

1. In the Case Details page, click **More Actions** and select **Change Status**.

The **Change Status** dialog appears.

2. In the **Status** list, select **Closed**.

3. Select a disposition.

Choices for the disposition are the following:

■ Confirmed Fraud

- Duplicate
- False Negative
- False Positive
- Issue Pending
- Issue Resolved
- Not Fraud

4. Enter a note describing the issue.

   You can select from existing notes, or enter a new note, or both.

   Existing notes to choose from are the following:

   - Issue Resolved
   - Issue Not Resolved
   - Old Case Cleanup
   - Duplicate Case
   - Other

5. Click **Submit**.

   A confirmation dialog is displayed.

6. Click **OK** to dismiss the confirmation dialog.

**Closing a Case Example**

An investigator finishes investigating a situation and determines that the customer was mistaken, there was no fraud. He uses the change status action to close the case and give a disposition of "not fraud".

### 5.6.4.2 Closing Multiple Cases

To close multiple cases:

1. In the Navigation tree, double-click **Cases**. The **Cases Search** page is displayed.

2. In the Search Results table, select the cases you want to close.

3. Click the **Bulk Edit** button.

4. Select **Closed** as the status.

5. Select the disposition and enter notes.

6. Click **Save**.

7. Click **OK** to dismiss the Confirmation dialog.

## 5.6.5 Bulk-Editing Agent Cases

To change the case settings for multiple cases at once:

1. In the Navigation tree, double-click **Cases**. The **Cases Search** page is displayed.

2. Select the cases you want.

3. Click **Bulk Edit**.

> **Note:** For out-of-the-box OAAM roles, the **Bulk Edit** button is disabled for the Investigator role and enabled for the Investigation Manager role.

4. Change the case settings you want and add notes.

   The **Close** action is allowed regardless of severity.

   Severity is editable regardless of status. You can also change the severity of cases irrespective of their Closed status.

5. Click **OK** to perform the bulk edit.

   A confirmation dialog appears with a message that the bulk editing operation was performed successfully. If you are closing a case and there are Agent cases that were already in the Closed status at the time of the bulk edit operation, a message appears, saying that the Agent cases have to be in the New or Pending status for a bulk close action to be executed.

6. Click **OK** to dismiss the dialog.

   When you refresh the search, the status is shown for those cases in the results.

"Last Case Action" on the Search page is not updated immediately after a bulk edit. It is updated when you launch the Search page again.

## 5.7 Linking and Unlinking Suspected Sessions to a Case

You can link sessions to the cases belonging to the users that belong to the organizations that you have access to.

### 5.7.1 Linking Sessions

If the Investigator feels that sessions are involved in the product security, he can search for those sessions, select them (you can see the sessions of only those groups to which you have access) and link them to the case with linking notes and descriptions.

To link sessions:

1. On the Case Details page, click the Linked Sessions tab.

2. Click the Link Sessions icon.

*Figure 5–2   Links Button*
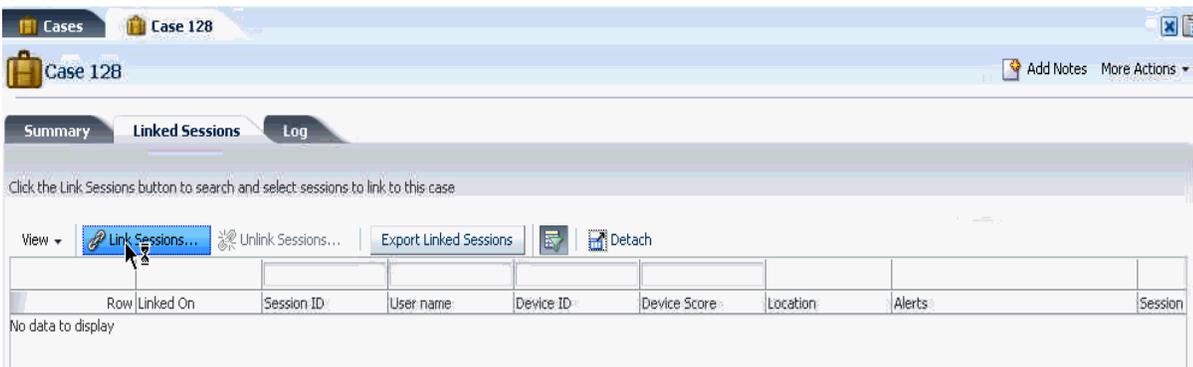


A Linked Session dialog opens where you can find the sessions to add.

**3.** Filter sessions on Session ID, User Name, IP Address, Device ID, and Location and specifying a specific login time range.

*Figure 5–3   Linked Sessions Search*



**4.** From the results, select the sessions to link to this case and click **Next**.

You can select one or more sessions to link at a time. These are the sessions that you think are part of the case that needs investigation.

A dialog appears showing that the sessions that can be linked to the case.

*Figure 5–4   Add Notes About Linking*
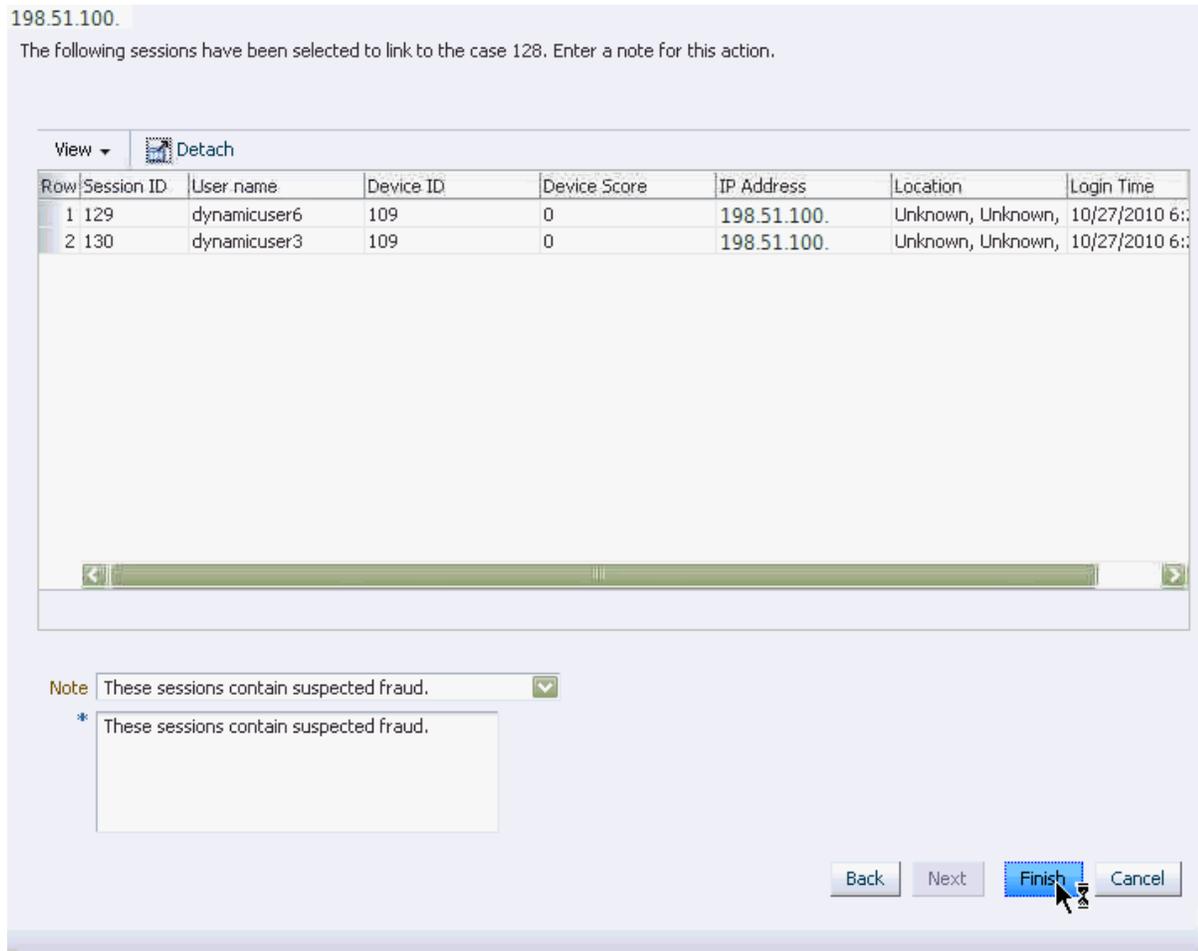


5. In the Notes field, select a note from the Note list or enter a note between 1 and 4000 characters into the text box to describe why you are linking the sessions.

6. Click Finish.

   The sessions are linked to the case and appear in the Linked Sessions tab.

## 5.7.2 Export Linked Session for Further Analysis

The Investigator can select one or more linked sessions and export them as MS-Excel document (XLS) for further analysis. Only MS-Excel document export is available.

The maximum number of linked session you are allowed to export is pre-configured for 1000. If you want to change the limit, you must edit the following configurable property:

```
oaam.xls.case.linkedsession.export.row.upperbound=1000
```

To export linked sessions for further investigation and analysis:

1. In the Case Details page, click the Linked Sessions tab.

   The Linked Sessions page opens, listing all the linked sessions.

2. Select the linked sessions you want and click Export.

3. Select Save Export File, browse for the location for file to be saved and click Export.

The sessions are exported with the following details:

- Row

- Date and time the session was linked

- Session ID

- User Name

- Device ID

- Device score

- Location

- Alerts

- Session date

- Notes

### 5.7.3 Unlinking Linked Sessions

If they feel that the linked sessions are not relevant to the case, an Investigator can unlink them from the case.

To unlink linked sessions:

1. On the Case Details page, click the Linked Sessions tab.

2. Click the Unlink Sessions icon.

The Unlink Sessions dialog opens, listing all the selected sessions to be unlinked.

3. Search for and select the linked sessions to unlink and press Next.

A dialog appears showing that the sessions have been unlinked from the case.

4. Enter notes about why you are unlinking the session.

5. Click Finish.

The sessions are unlinked from the case.

## 5.8 Agent Case Feedback

Agent case feed back closed findings into the risk engine to improve accuracy of future evaluations automatically.

For example, an investigator creates an Agent case and links several fraudulent sessions to it. Later, the investigator closes the case with a disposition of confirmed fraud. A predictive model is rebuilt every "n" hours to take into account data from sessions linked to cases with a confirmed fraud disposition. Investigators can determine the frequency of rebuilding the models. Each session in the system is compared to see how close it is to the fraudulent ones. The closer the match the higher the risk. An example evaluation would be, was the probability more than 50% that this login session is fraudulent based on all sessions linked to confirmed fraud cases?

## 5.9  Configuring Agent Case Access

By default only Investigators and Investigation Managers have access to create Agent cases. The property for investigator access is
`oaam.permission.creatagentcase=oaam.perm.create.case.type.agent`

To give a CSR access to Agent cases, configure the property as follows:
`oaam.permission.creatagentcase=oaam.perm.create.case.type.csr`

After setting the property, the CSR should have full access to create agent cases.

## 5.10  Configuring Expiry/Overdue Behavior for Agent Cases

The expiry/overdue behavior can be configured using the Properties Editor.

Agent Cases have a default expiration date of 24 hours from the date of creation.

Information to change the default behavior is provided below.

### 5.10.1  Set "Overdue" Behavior for Agent Cases (Default Setting)

To set "expiry/overdue" behavior for Agent cases, modify the following properties as shown below.

```
customercare.case.expirybehavior.enum.agentcase.behavior = overdue
customercare.case.expirybehavior.enum.agentcase.label = Overdue
customercare.case.expirybehavior.enum.agentcase.durationInHrs = 24
customercare.case.expirybehavior.enum.agentcase.resetonaccess = true
```

### 5.10.2  Disable "Overdue/Expiry" Behavior for Agent Cases

To disable the "overdue/expiry" behavior for Agent cases, modify the following property as shown below.

```
customercare.case.expirybehavior.enum.agentcase.behavior = none
```

> **Note:**   You do not need to change the other parameters.

### 5.10.3  Set "Expiry" Behavior for Agent Cases

To set "expiry" behavior for Agent cases, modify the following properties as shown below.

```
customercare.case.expirybehavior.enum.agentcase.behavior = expiry
customercare.case.expirybehavior.enum.agentcase.label = Expired
customercare.case.expirybehavior.enum.agentcase.durationInHrs = 24
customercare.case.expirybehavior.enum.agentcase.resetonaccess = false
```

## 5.11  Agent Use Cases

Common agent use cases are listed below.

### 5.11.1  Agent Creation

Agent use cases are provided below. Groups for the examples are presented in the following chart.

*Table 5–7    CSR Access*

| Organization | Application Users | Admin Users |
|---|---|---|
| Default | | |
| | ■  demouser1 | ■  democsr1 |
| | ■  demouser2 | ■  democsr2 |
| | ■  demouser3 | ■  democsr3 |
| Org2 | | |
| | ■  org2user1 | ■  org2csr1 |
| | ■  org2user2 | ■  org2csr2 |
| | ■  org2user3 | |
| Both organizations | | |
| | | ■  supercsr1 |
| | | ■  supercsr2 |
| No organization | | democsrm1 |

**Current Owner is the Agent who is Working on the Case Currently**

The Current Owner is the agent who is working on the case currently.

1.  A manager named "democsrm1" logs in.

2.  He searches for the case by Notes.

3.  He opens the case.

4.  As soon as he opens the case

    a.  The Current Owner changes from "democsr1" to "democsrm1."

    b.  The Created By field still shows "democsr1."

    c.  The status of the case is "Pending."

5.  Next, the CSR Manager can perform the necessary actions such as granting a temporary allow, performing challenge question resets, and other actions.

**CSR Escalates a Case to an Agent Case**

CSR escalates a case to an Agent Case.

CSR named "democsr1" has permission for group "Default."

1.  He logs in to the system.

2.  He creates a new case

    ■  He selects the Organization ID, "Default."

    ■  He creates the case for "demouser2."

    ■  He selects the severity and gives the description, "fraudulent activity."

3.  He escalates the case to an Agent case and adds notes.

4.  Now the CSR, "democsr1" does not have permissions to see the details of the case.

**Agent Cases Escalated from CSR Case has User Details**

User details are shown in escalated Agent cases.

1.  An Investigator, "demoinvest1" logs in to the system.

2. He searches for Escalated cases by filtering on Escalated.

3. He opens the case.

    a. Case Status changes from "Escalated" to "Pending."

    b. Created By field still shows "democsr1."

    c. Current Owner shows "demoinvest1."

    d. User details are also displayed because this is not a user less case, but a CSR case that was escalated to an Agent case

    e. Log shows that the case was created, then escalated, then accessed, and then the status changed.

### Investigator can Create Agent Cases

A case can be created by an Investigator.

1. The Investigator, "demoinvest1," logs in to the system.

2. He creates a case

- He selects the Organization ID.

- He does not have to select a user because this is a user less case.

- He selects the severity.

- He gives a description.

The Case Details page appears.

- The Case Status is "Pending."

- The Created By field shows "demoinvest1."

- The Current Owner field shows "demoinvest1."

- User details are not shown because this is a user less case.

### Investigator Can Create Agent Case for a Different Organization ID

Investigator can create Agent case for a different Organization ID if he has permissions to access multiple organizations. In most scenarios only the Investigation Manager has access to multiple organizations.

1. The Investigator, "demoinvest1," logs in to the system.

2. He creates a case

- He selects a different Organization ID.

- He selects the severity.

- He gives a description.

3. He views the logs, which shows that the case was created.

### Concurrent Access of Case

An example of when two agents try to open a case is described below.

1. demoinvest1 logs in and searches for a case with status "New."

2. He can see the case, Case ID 132, in the results.

3. Another user demoinvest2 logs in and searches for a case with status "New."

4. He can also see the case, Case ID 132, in the results.

5. demoinvest2 opens the case and the status changes to "Pending."

6. demoinvest2 is the current owner of the case.

7. demoinvet1 still sees the case as "New" in the results.

8. He tries to open this new case but a message appears saying that demoinvest2 is the current owner of the case and he can choose to continue or cancel.

9. If he chooses to cancel, nothing happens and demoinvet2 remains the current owner.

10. If he chooses to continue, he becomes the current owner and the status of the case is "Pending."

**View Overdue Cases**

The Investigator searches for Agent cases with Shown Only Expired as the Expired filter. The cases with dates and time displayed in red in the Expiration Column are overdue cases.

**Search Cases By Action**

Users can search both CSR and Agent cases based on actions that were taken in them. An example is provided below:

Yesterday jsmith called customer service claiming to have lost money out of his account. The CSR escalated the case and told jsmith he would be contacted within 24 hours. jsmith calls back 36 hours later to see why he has not been contacted. The CSR needs to view the case escalated yesterday for jsmith. He searches cases for jsmith with an "Escalate" action and ones that are not overdue in the last 48 hours.

## 5.11.2 Investigation Workflow Scenario - Blocked Login Attempts

Agent type cases are used by fraud investigators to do the following:

- Collect investigation findings for audit including which investigators have worked on a case

- Manage the lifecycle of an investigation including severity, status, ownership changes, time to resolution, dropped/lost cases and resolution

- Feed back closed findings into the risk engine to improve accuracy of future evaluations automatically

- Export findings to Excel for external records or processes

A fraud investigator can quickly view the data involved in an incident and quickly locate related situations by easily harnessing the complex data relationships captured by OAAM. Search and detail pages provide fraud investigators the ability to:

- Drill into individual sessions to see the exact chain of events that led to an alert

- View and search for complex relationships between different data types

- White/black list entities "on the fly" without leaving the investigation flow

  This feeds back into risk evaluation. For example, a high risk device group.

- Link session data to a case to further narrow the investigation

A security administrator configures an action to create an Agent cases when specific rules trigger. These autocreated cases require a review of the transaction. The details pages contain the information needed by the investigator in order to accomplish this task. An example workflow is shown below for an autocreated case.

### Search for New Autocreated Agent Cases

John is a fraud investigator for the bank. John searches for new Agent cases dynamically created as a result of blocked access requests.

**Best Practice**: Filter the time-stamp column so the oldest case is on top.

*Figure 5–5   Searching for New Autocreated Agent Case*



### Review the Generated Alerts

John opens case 109 the oldest case in the listing to start working on it. Automatically the case status changes from **New** to **Pending** and the current case owner becomes John. Other investigators can now see that this case is actively being worked (since the case has an owner, John, and the status is not new, but pending). When case 109 was automatically created the session which was blocked was linked to the case so all the session data is captured and ready for review. This includes a full set of the alerts triggered in the session. This example show a session in which five different alerts were triggered. John can easily read the alert messages to understand what was going on in this situation. The highest alert was generated because the access attempt was from an IP known to be an anonymizing proxy. The bank security policy restricts banking while utilizing an anonymizing proxy as they are often used by criminals to hide their true geographic location.

*Figure 5–6   Reviewing Alerts*



### Review User Accounts Used From High Risk IP Address

John clicks the IP address to drill in on the location to investigate further. Note Table 5–6, " Log Search Filters" shows the most severe alert as one that concerns an IP address (an anonymizing proxy). This opens the IP address details screen in an adjacent user interface tab. John selects the users tab to see what user accounts have been utilized from this high risk IP address. He can see that there are four different bank users potentially affected by the activity originating from this location.

*Figure 5–7   Reviewing User Accounts Used From IP Address*
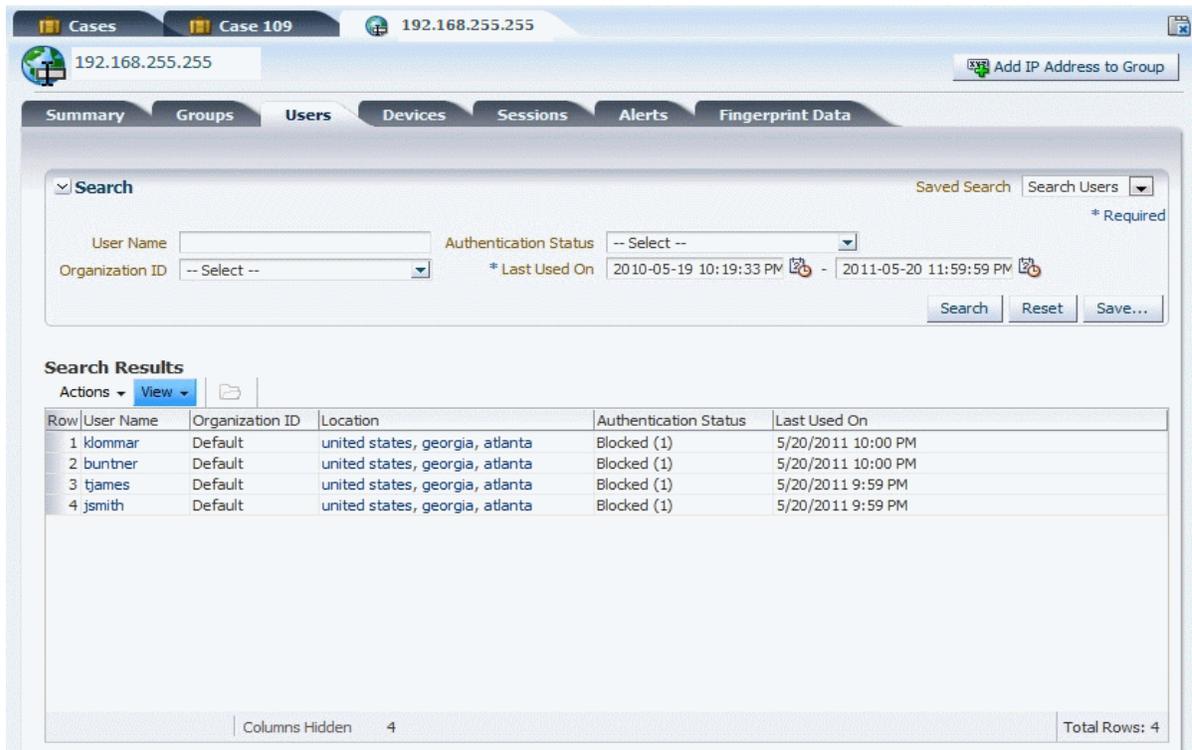
**Link Sessions to Agent Case**

John clicks the sessions tab of the IP details screen to list sessions from this IP address.

*Figure 5–8   Searching for Sessions to Link to Agent Case*



He selects them all and links them to case 109 that he is working on. This way he collects the data he has found along with notes as to why he did this. In this case all the sessions had been blocked but if there were some sessions that had not been blocked then linking those sessions to the case for further follow up is extremely useful since without the data cross referencing ability of the details screens such a situation may have gone undetected.

*Figure 5–9   Linking Sessions to the Agent Case*
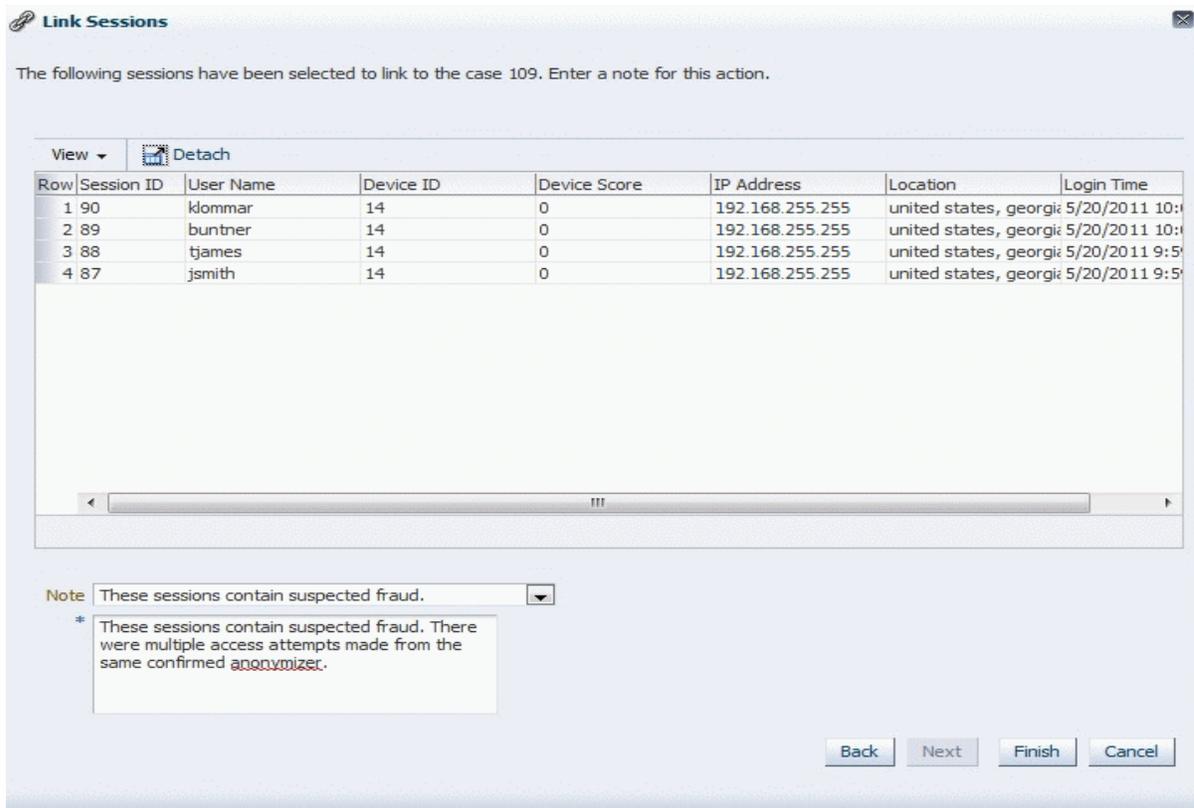


### Review Linked Sessions in Agent Case

Now all data from these linked sessions is captured in case 109. John can see that the same device (#14) was used in all these blocked access attempts.

*Figure 5–10   Review Linked Sessions in Agent Case*
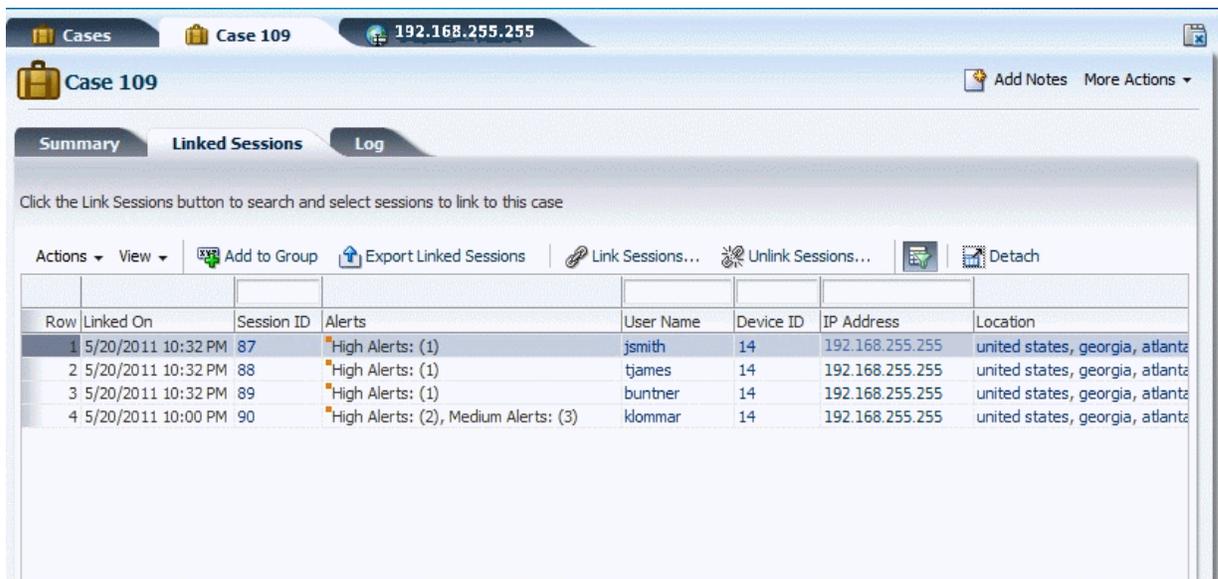
**Review Details of the Sessions Parameter in Question**

John clicks device 14 to open the device details screen. In the device details an investigator can also see data relationships and sessions for this device but can as well view the fingerprinting details of the device itself. For example, the browser locale used.

*Figure 5–11  Viewing Details About the Sessions Parameter*



**Review Alerts From Activity Involving the Session Parameter**

John opens the alerts tab to view the types of alerts and frequency of each generated from activity by involving this device. For example he can see the aggregate count for the anonymizer alert is four.

*Figure 5–12   Reviewing Alerts Involving the Session Parameter*
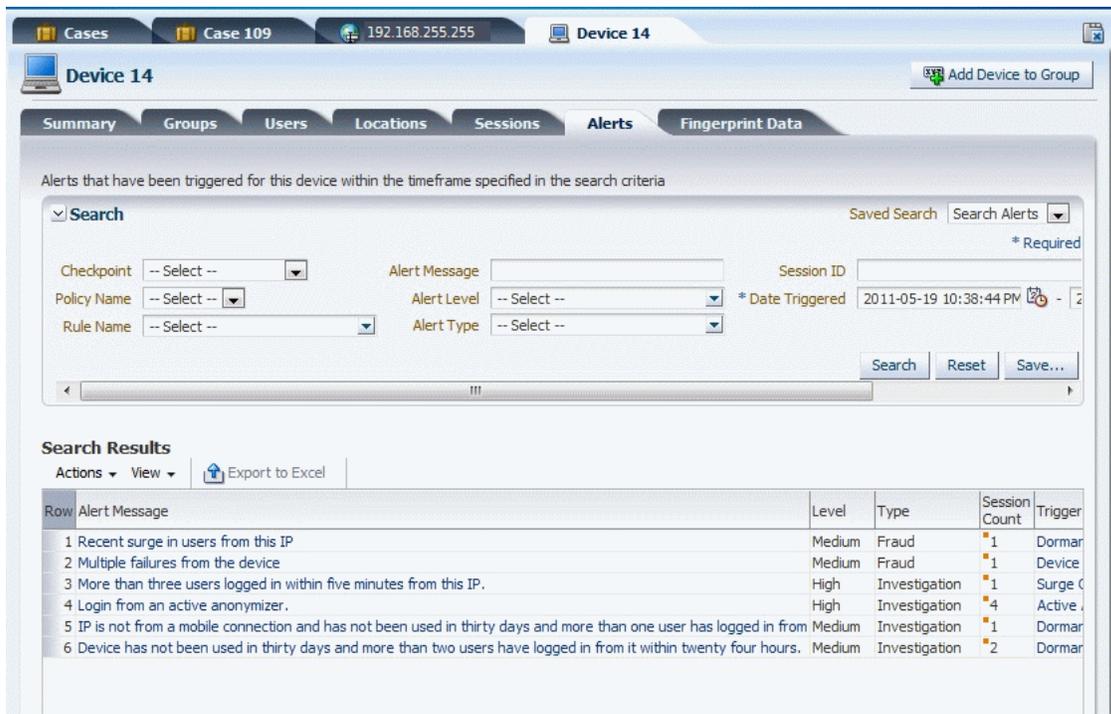


### Export the Linked Cases to Excel

John follows up with phone calls to the four affected customer account holders to further confirm that they were not the ones attempting these blocked attempts. Feeling he has investigated this incident to the fullest and confirmed fraud John is ready to close the case and move on to the next incident. Before closing the case John exports the linked sessions to Excel.

*Figure 5–13   Exporting Linked Sessions to an Excel Sheet*
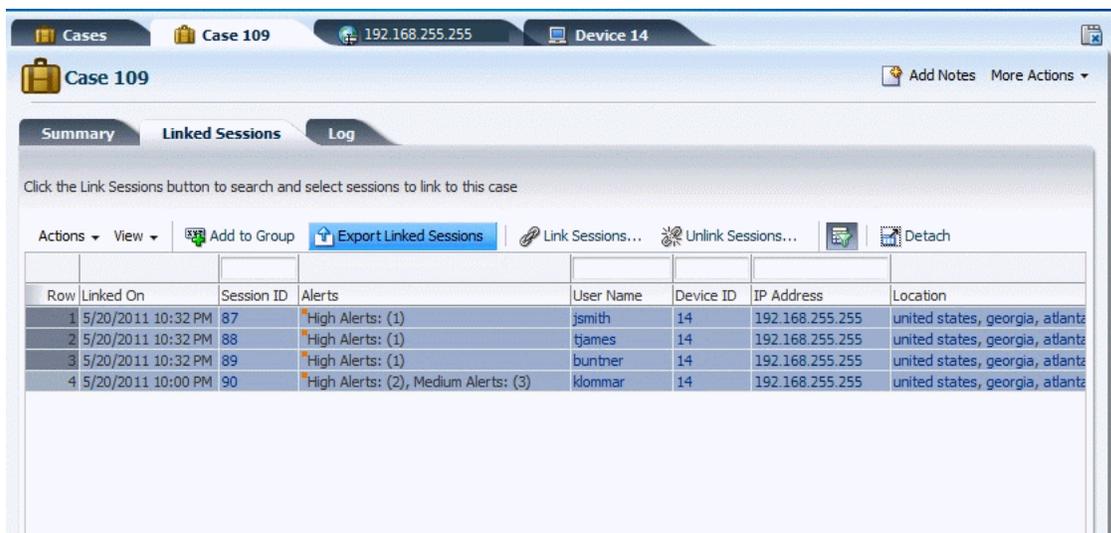


He exports the sessions so that he may furnish the evidence to federal law enforcement as part of an industry wide program.

*Figure 5–14 Evidence to Show to Authorities*



### Add Session Parameters to a Restricted Group

John feels confident that this device has only been used for fraudulent access attempts so he determines it should be blacklisted. Directly from the details screen John adds the device to the Restricted Devices group. This ensures it cannot be used to access online banking even if the other session data seems valid and no other rules trigger. This is very important as fraudsters often hit multiple times testing the security of an application to see how they can get around it. Device fingerprinting can be the one data point that stays the same across fraudulent attempts.

*Figure 5–15 Adding Session Parameters to Restricted Group*

### Close the Case

John closes the case as confirmed fraud with notes summarizing his findings. His manager or auditors can view a full log of case activity including actions taken, notes and individuals involved.

*Figure 5–16   Closing Agent Case with Notes*



Since the case was marked as confirmed fraud the combinations of specific data found in the fraudulent access requests are automatically consumed by the risk evaluation engine to "teach" it what fraud looks like. This helps improve accuracy of future risk evaluations. Likewise, if John has found that the alerts he saw were not the result of fraud he would have closed the case and marked it as not fraud. This would also adjust future risk evaluations to reduce false positives.

*Figure 5–17    Agent Case Search Results*



## 5.11.3  Investigation Workflow for CSR Escalated Agent Cases

A CSR Manager escalates a CSR case. Matt is a fraud investigation agent specializing in customer specific security issues. He searches for all cases with the Escalated case status. Best practice is for investigators not to open cases that other investigators are working on. The first time an investigator accesses a case, the status changes to "Pending" automatically. This allows investigators to know if another investigator is already working on the case. Matt opens the escalated case. The status automatically changes from Escalated to Pending and the Current owner becomes Matt. Best practice is to open the escalated case and view the logs for notes entered by the CSR and CSR Manager. He sees they escalated the CSR case to an agent case because they suspected fraud activity. Because the case originated from a customer service case, it contains specific user information in the details. Matt looks at the case details and notes that jsmith is the user. He writes down the user ID because he needs it to search for sessions. Matt navigates to the Linked Sessions tab and opens Linked Sessions to search for sessions by the user ID, jsmith. jsmith has sessions so Matt looks for the most recent session by filtering on the date and the timestamp. Matt wants the most recent one because it caused the escalation. He reviews the alerts messages to understand what occurred. The highest alert was generated because the access attempt was from an IP known to be an anonymizing proxy. Matt clicks the IP address to drill in on location logins to investigate. He looks at other locations from the past to determine if a fraud potentially occurred. Since he has more questions, he calls the actual user, jsmith, and talks to him and takes notes. When Matt is satisfied his conclusion, he closes the case with a disposition.

## 5.11.4  Investigation Workflow for Manually Created Cases

Harry reads about a new type of fraud in an online security magazine. He decides to configure and run new reports to see if the attack has been attempted at Dollar Bank. He finds three sessions that seem suspicious. He wants to investigate further so he

creates an Agent case and links these sessions to it. Harry picks some data points from the three sessions to drill in on. On the details screen one of the devices in the linked sessions is returning a large amount of sessions for a single user ID. His shift is almost over but this investigation has enough urgency that he would like another investigator in the next shift to continue investigating the case. Harry adds some notes to the case requesting that someone keep working on this case and any insights he has. Harry changes the status of the case to "attention required" so another Investigator picks it up.

1. Fraud Investigator opens the OAAM Admin Console and sees only the appropriate user interface views and controls afforded his role.

2. Fraud Investigator creates a case.

3. Fraud Investigator links the session.

4. Fraud Investigator repeats steps 2 and 3 as required

5. Fraud Investigator changes the case status to "attention required."

6. Fraud Investigator adds notes.

## 5.11.5 Investigation Workflow for Auto-Created Cases

Gary is a Fraud Investigation Agent for Dollar Bank. Gary searches for a new case to work on. He performs a search for all cases with new status, no current owner and filters the view by cases with least time to overdue at the top. Gary selects the first case, looks at the alerts and other data in the linked session. He then searches to find other sessions from North Korea. One other session is returned when he searches for the last six months. Gary links this second session to the case so relationships based on data from both of the sessions can be used to investigate. Gary notices that the two linked sessions were from the same device. Gary continues the investigation by looking into other sessions from this device in the past year. He finds there is another session from this device that says it was from China. He links that session as well. Each of the three sessions used a different IP address. Next Gary individually looks for sessions from each IP. Two of the IPs was only used in those sessions. The third IP from China had 178 sessions in the last three months. He wants to see the users potentially affected by this situation so he opens the IP details screen and views the users tab. A listing of all the users with details for each is shown. Gary looks into the identity management product to investigate each user to see if any have contact information in China. None of them do, all are Americans living in the continental US. Gary exports the list of user to XLS and contacts the customers who accounts were being used to ask a few questions. He finds that none of them had been in North Korea or China so he enters the conversations in the case notes. He asks them to change their passwords and resets their challenge questions. He also adds them to a victim watch list group and the device to a high risk watch list. Gary then closes the case with a confirmed fraud disposition.

1. Fraud Investigator opens the OAAM Admin Console and sees only the appropriate user interface views and controls afforded his role.

2. Fraud Investigator searches cases.

3. Fraud Investigator opens a case.

4. Fraud Investigator links session.

5. Fraud Investigator repeats step 3 and 4 as required.

6. Fraud Investigator generates list view of users affected.

7. Fraud Investigator adds users to victim list.

8. Fraud Investigator adds device to black list.

9. Fraud Investigator closes case.

## 5.11.6 How Users Use Agent Cases for Investigation

Oracle Adaptive Access Manager allows the creation of Agent cases to make forensic investigations quicker, easier and more successful.

An Agent case is created when a suspicious activity or fraud scenario is detected and needs investigation.

An example of how an Investigator uses Agent cases is shown below.

1. The Investigator receives automated high alerts of the type, "Fraud."

2. The Alert message notifies him that there are potentially suspicious sessions from North Carolina.

3. The Investigator immediately logs in to OAAM and searches sessions based on various filter criteria, such as the sessions from North Carolina.

4. He determines the sessions that needs investigation.

5. The Investigator creates an Agent case and start the investigation.

6. He selects these sessions and links them to the case.

   As part of the linking the Investigator enters notes describing why the sessions were linked. The case log records the notes as well as the user who performed the link action. These sessions stay linked to the case unless they are unlinked by an investigator or manager.

7. The Investigator looks at the city and state in the Location Details page because many of the suspicious sessions occur in North Carolina.

8. Once the Investigator comes up with a conclusion, he closes the case with a disposition.

## 5.11.7 Associating Fraud Sessions with a Case for Investigation

The following section outlines the steps to associate fraud sessions with a case for investigation.

**Before You Begin**

Ensure that you have the proper permissions to create and work with Agent cases.

**Associating the Fraud Sessions with a Case for Investigation**

You receive automated high alerts of the type, "Fraud," and the alert message notifies you that there are potentially suspicious sessions.

1. Log in to the OAAM Admin Console and search for sessions based on various criteria.

   For example, you might search for all sessions that were blocked in the last **12 hours** with **High** alerts (sessions filtered by **Time**, **Alert Level** and **Action**).

2. Go to the Session Details page to collect more information about the session you are interested in.

   You could look at:

   ■ Outcomes of checkpoints

- Policies and rules triggered

As an investigator, you are interested in why a particular rule triggered. For example, you might look at which policy and rules triggered the alert.

Information can be gathered by looking at these details. For example, a user who successfully went through Pre-Authentication and Post-Authentication checkpoints knew the password and the questions and answers and there fore, there is a good chance that he is a valid user. On the other hand, a user who attempted to answer the questions twice and succeeded in providing a correct answer on his third attempt might be considered suspicious. This user did not know the answers right away so there is a chance that he may be a fraud trying out new answers.

3. In the Policy Explorer in Session Details, view the runtime values for each one of the policies and rules that were triggered.

For example, if a rule triggered that showed that the user had logged in from a country that he did not usually log in from, you would want to look at the runtime details to see which country he logged in from.

The Policy Explorer shows the policies that were triggered, the condition parameters, and the actual values.

4. Determine the sessions you need to investigate.

5. Create an Agent case and start the investigation.

6. Search and select these sessions and link them to the case.

As part of the linking enter notes describing why the sessions were linked. The case log records the notes as well as the user who performed the link action. These sessions stay linked to the case unless they are unlinked by an investigator or manager.

7. Identify the relationship between the sessions and view the appropriate detail pages.

For example: If the suspicious sessions used the same device, view the Device Details page. If the suspicious sessions are from the same location, view the Location Details page. If the suspicious sessions are from the same user, view the User Details page. If the suspicious sessions all used a Spanish browser, view the Fingerprint Details page.

   a. View Location Details page.

   b. View Device Details page.

   c. View Fingerprint Details page.

   d. View Alert Details page.

   e. View User Details page.

8. Analyze the sessions and when you reach a conclusion, close the case with a disposition.

## 5.11.8  Listing the Cases that I Am Currently Working With

Both CSR and Agent type cases can be searched based on the current owner. This search filter finds cases for which the last action performed was by the user you are searching.

**Before You Begin**

Ensure that you have the proper permissions work with cases.

**List Cases I'm Currently Working On**

1. Log in to the OAAM Admin Console.

2. As a CSR or CSR Manager: In the Cases search page, search for the cases you are currently working on by specifying the following criteria in the search filters:

*Table 5–8   CSR Searches for Cases Working On*

| Filter | Value |
| --- | --- |
| Current Owner | Search by your user name. (The agent who performed the last action) |
| Case Status | Pending |
| Expired | Hide Expired |

3. As an Investigator: In the Cases search page, search for the cases you are currently working on by specifying the following criteria in the search filters.

*Table 5–9   Investigator Searches for Cases Working On*

| Filter | Value |
| --- | --- |
| Current Owner | Search by your user name. (The agent who performed the last action) |
| Case Status | Pending, Escalated |
| Expired | Hide Expired |

## 5.11.9  Marking One or More Sessions as Confirmed Fraud

The following section outlines the steps to mark one or more sessions as confirmed fraud. Included are references to other sections where you can find specific information.

**Before You Begin**

Ensure that you have the proper permissions to create and work with Agent cases.

**Mark One or More Sessions as Confirmed Fraud**

To mark a session as Fraud/Not Fraud, create an agent case link the session and close the Agent case with Disposition as either "Confirmed Fraud" or "Not Fraud".

1. Log in to the OAAM Admin Console as an Investigator.

2. Create an Agent case. Refer to Section 5.5.5, "Creating an Agent Case Manually."

3. Link sessions to the case. Refer to Section 5.7.1, "Linking Sessions."

4. Change the severity of the case to High. Refer to Section 5.6.2, "Changing Severity Level of a Case."

5. Close the case with Disposition as "Confirmed Fraud." Refer to Section 5.6.3, "Changing Status of a Case."

## 5.11.10  Closing a Case

The following section outlines the steps to close a severity of High.

**Before You Begin**

Ensure that you have the proper permissions to work with cases.

**Close a Case**

To close a case:

1. Log in to the OAAM Admin Console.

2. Navigate to the Cases search page. Refer to Section 5.3, "Opening the Case Search Page."

3. Open the Case Details page. Refer to Section 5.5.3, "Viewing Agent Case Details."

4. Change the severity of the case to High. Refer to Section 5.6.2, "Changing Severity Level of a Case."

5. Change the status of the case. Refer to Section 5.6.3, "Changing Status of a Case."

6. Close the case with a disposition. Refer to Section 5.6.4.1, "Closing a Case Manually."

## 5.11.11 Closing Multiple Cases

The following section outlines the steps to close multiple cases.

**Before You Begin**

Ensure that you have the proper permissions to work with cases.

**Close Cases**

To close multiple cases:

1. Log in to the OAAM Admin Console.

2. Navigate to the Cases search page. Refer to Section 5.3, "Opening the Case Search Page."

3. Close multiple cases. Refer to Section 5.6.5, "Bulk-Editing Agent Cases."

## 5.11.12 Auto-Status Change (Escalated Cases)

Actor: Security Investigator/Security Investigator Manager

CSR case is created via one of the two possible flows (auto/manual).

1. CSR performs escalate case action. Case is turned into an Agent type case with a status of "Escalated".

2. Investigator searches for all the cases with "Escalated" status. He filters the results on the severity column so the highest severity cases are shown at the top.

3. He clicks one of the high severity case IDs in the list. Validation checks if the case still has "Escalated" status before opening the case screen and automatically changes the status to pending.

4. Case log displays creation, escalate action, access by user and status change to pending.

## 5.12 Best Practices and Recommendations

Best practices and recommendations are provided below:

- A Fraud Investigator looks into suspicious situations either escalated from customer service or directly from alerts.

- An Fraud Investigation Manager would want to see which cases need to be given attention by his team.

- A Fraud Investigation Manager must routinely search for overdue cases to make sure none of the cases are pending.

- If a customer suspects fraud, then the severity level assigned is "High." For example, 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. Anyone can change the severity of cases.

# 6

# Viewing Additional Details for Investigation

OAAM provides the capability to gather detailed information about the session parameters and to allow you to drill down further into the details involved in the session. The session parameters are users, devices, locations, alerts, and fingerprints.

## 6.1 Details Pages Overview

The investigators are assigned to perform fraud investigation and leverages all available data, knowledge, and expertise to determine if in fact there is fraudulent activity present.

The details pages provide additional details of session parameters such as user, device, location, alerts, and fingerprints and shows their relationships so that you can cross references on data points and drill in on related data.

The following are examples of related data:

- Administration groups to which the session parameters belong

- Sessions in which the parameter was used

- Success and failure login attempts for the parameters

- Policies and rules executed during those sessions

- Alerts generated for the session

- Fingerprint information

**Example of relationships between parameters:**

You can identify what devices a single user used, which particular location was the device used, which login attempts were successful, and how many users logged in from a particular location.

## 6.2 Details Page Structure

Each details page provides the following items:

- Summary of basic information such as ID, name, creation date, and other information

  For an example, refer to Section 6.11.1, "User Details: Summary Tab."

- Detail tabs for a view of the entity's relationship with other entities

  The relationships are shown through the tabs.

  For summaries of the tabs for each details pages, refer to:

- Links to details pages for more information
- Add to Group feature

## 6.3 Prerequisites

Prerequisites for viewing details pages are listed in this section.

### 6.3.1 Multitenant Access

To have access to details pages, ensure the multitenancy flag is disabled. If the user's role is a multitenant enabled role, he may not be able to access the details pages. If multitenancy is enabled, these users cannot access any of the details pages from the sessions page or sessions search. If the multitenancy flag is disabled, these users can access details pages from the sessions page or any sessions search if the link is available. CSRs do not have access to the sessions search or details pages.

### 6.3.2 View Transactions in Session Details

Before you can view transactions in the **Session Details** page, you must set the property to show transactions to true.

```
bharosa.trackeradmin.show.transaction.detail=true
```

Setting the property to `false` turns off the display for transactions.

Before using the details pages, check that the following properties are enabled.

```
oaam.admin.detail.ip.enabled=false
oaam.admin.detail.user.enabled=true
oaam.admin.detail.device.enabled=false
oaam.admin.detail.fingerprint.enabled=false
oaam.admin.detail.alert.enabled=false
oaam.admin.detail.challengecount.enabled
=false
```

## 6.4 Searching for Sessions

To search for sessions:

1. Log in to OAAM Admin as an Investigator.

2. In the Navigation tree, double-click **Sessions**. The **Sessions Search** page is displayed.

    Alternatively, open the **Sessions Search** page by:

    - Right-clicking **Sessions** in the Navigation tree and selecting **List Sessions** from the context menu.

■ Selecting **Sessions** in the Navigation tree and then choosing **List Sessions** from the **Actions** menu.

■ Clicking the **List Sessions** button in the Navigation tree toolbar.

*Figure 6–1   Sessions Search Page*
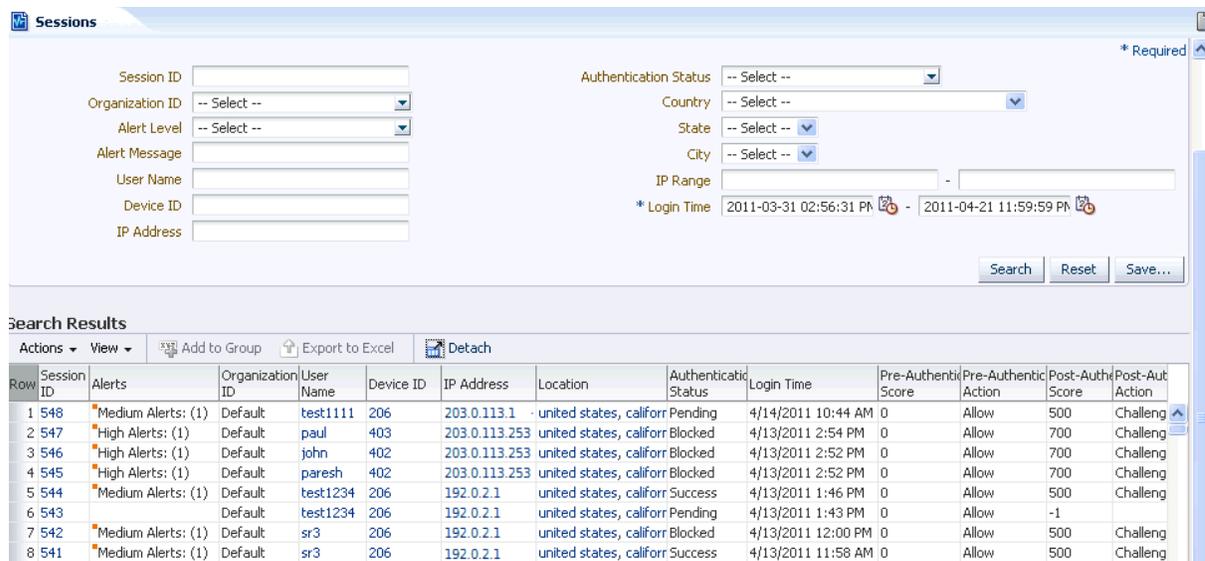


3. In the Sessions search page, narrow down the number of sessions that are returned by specifying criteria in the search filters.

For example, search through sessions in the last **12 hours** with **High** alerts and a **Blocked** or **Locked** authentication status (sessions filtered by **Time**, **Alert Level** and **Action**).

The filters are:

*Table 6–1   Session Search Filters*

| Filters | Description |
| --- | --- |
| Session ID | ID for the session. |
| Organization ID | Identifies the organization to which the user belongs. |
| Alert Level | Severity of the alert whether high, medium, low. |
| Alert Message | Text message configured in the alert. |
| User Name | Login name given by user to login. |
| Device ID | Uniquely identifies each device and is autogenerated by the application. |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Country | Country ID |
| State | State ID. The State list is dynamically populated with respect to what has been selected for Country. For example, if United States is selected, whatever states are available for that country are shown under States. |

*Table 6–1   (Cont.)  Session Search Filters*

| Filters | Description |
|---------|-------------|
| City | City ID. The City list is dynamically populated with respect to what has been selected for in Country and State. |
| IP Range | Range of IP addresses |
| Login Time | The time the customer logged in to perform the transaction. For example, 5/11/09. |

Click the **Session ID**, **User Name**, **Device ID**, **IP Address**, **Location**, and **Alert Message** to open the corresponding details pages to view additional information.

> **Note:**   If the checkpoint is not run, the Pre-Authentication or Post-Authentication displays a score of -1.

*Table 6–2   Search session results*

| To open the Details page | Click this link |
|--------------------------|-----------------|
| Session Details page | Session ID link |
| | Click the Session ID link from the sessions listing or other pages to open the corresponding Session Details page, which shows consolidated information about the session. |
| Alert Details page | Alert message links from other pages (session details, other detail pages, and Agent pages) |
| | Click the alert message links from other pages (session details, other detail pages, Agent pages) to open the Alert Details page. The Alert Details page provides information on the message, level, type of the message and cross references on other data types such as user, device, location, sessions, browser, operating system, locales, and others. Additionally, information is provided about the way/ways in which the alert were generated. |
| User Details page | User Name or UserID links from other pages |
| | Click the User Name or UserID links from other pages to open the User Details page, which shows additional details regarding that user. |
| Device Details page | Device ID link in the session details or other listing pages |
| | Click the Device ID link in the session details or other listing pages to open the corresponding details page. This page displays details for a device including cross references on other data types such as user, location, alerts, browser, sessions, full list of fingerprint data, and so on. |

*Table 6–2   (Cont.)  Search session results*

| To open the Details page | Click this link |
|---|---|
| IP Address Details page | IP Address links from sessions listing or other pages. |
| | Click the IP Address links from the sessions listing or other pages to open the corresponding IP Address Details page, which shows additional details regarding that IP location. |
| Location Details page | Country, State or City links from the sessions listing or other pages |
| | Click the Country, State or City links from the sessions listing or other pages to open the corresponding Location Details page, which shows additional details regarding that location. |
| Fingerprint Details page | Flash Fingerprint ID or Browser Fingerprint ID links from the session details or listing page |
| | Click the Flash Fingerprint ID or Browser Fingerprint ID links from the session details or listing page to open the Fingerprint Details page. The Fingerprint Details page provides basic information about the Fingerprint; the data collected during Device Fingerprinting; lists of users, devices, and locations used; and a list of login sessions in which the fingerprint was generated for a particular period. |

You can launch a details pages from another details page, up to a maximum of 10 tabs. The details page tabs also contain hyperlinked parameters, which can launch the details pages.

> **Note:**   When multitenancy is enabled, investigators do not have access to details pages from anywhere in the OAAM Admin Console.

## 6.5  Export Sessions to Excel

An export option is available on details pages and tabs for exporting sessions information to Excel. To export sessions information for further investigation:

1.  In the details page or tab, search for and select the sessions to export.

2.  Click the **Export to Excel** button.

3.  Click **Save File** or **Open** with and click **OK**.

    The Excel sheet shows information on the Row, Session ID, Alerts, Organization ID, User name, Device ID, IP Address, Location, Authentication Status, Login Time, Pre-Authentication Score, Pre-Authentication Action, Post-Authentication Score, Post-Authentication Action, Client Type, User ID, and Internal Session ID.

## 6.6  Add to Group

An Add to Group feature is available in Search sessions, session details, and each details page. While searching results, insights can be saved and used later for rebuilding predictive models, further investigation and rules evaluation. Add a sessions parameter to a group or create a group and add the sessions parameter to it, or remove a sessions parameter from a group, using the **Add to Group** button from the sessions pages (sessions search results and Session Details page).

One or more data points of various types can be easily selected in search results and added to an appropriate group.

Only Security Administrators, System Administrators, and Investigators have access to the **Add to Group** command.

*Table 6–3    Add and Remove from Group*

| Feature | Description |
| --- | --- |
| Add sessions parameter to sessions parameter group | Select a sessions parameter group from a list of parameter groups with which the parameter is not already associated and add the parameter to it. A User Group can be either a User ID or User Name group type.

A parameter cannot be added to the same parameter group multiple times with the exception of the alert.

An alert can be added to an Alert Group multiple times, since whenever an alert is added to an Alert Group, a new instance of the existing alert is created and added to the group. |
| Create a new sessions parameter group and add parameter to the newly created group. | Add a new parameter group and add the parameter to it. A user group can be of either User ID or User Name group type. |
| Remove parameter from parameter group | Select multiple parameter groups with which the parameter is already associated and remove the parameter from the selected groups. Note: Removing users from Organization ID is not recommended. |

Instructions for adding sessions parameters is provided in the following sections.

## 6.6.1 Add to Group From Sessions

To add a sessions parameter from sessions to an existing group

1.  Select sessions of interest from the search results.

2.  Click the **Add to Group** button.

    The Add to Group dialog is displayed.

3.  Choose the type of data to add to a group and click **Next**. Choose only one data type at a time.

    - Device

    - User name

    - IP Address

    - Country

    - State

    - City

4.  Search and select existing groups for adding the device to and click **Next**.

5.  Items to be added to the group are listed below. To go back and change the items, click the **Back** button. To proceed with adding these items, click the **Finish** button.

To add a sessions parameter to a group that is being creating:

1.  Click **Create New group** to create a new group to add the device to.

2.  On Add to Group dialog, enter:

    - Group Name

    - Cache Policy

    - Description

3.  Click **Next**.

4. Items to be added to the group are listed. To go back and change the items, click the **Back** button. To proceed with adding the items, click the **Finish** button.

## 6.6.2 Add to Group from Details Pages

To add a sessions parameter to a group:

1. Select a row containing one or more session parameters (user, Device ID, IP, and so on).

2. Click the **Add to Group** button in the upper right corner.

The Add to Group dialog appears with the following search filters:

*Table 6–4    Add to Group Dialog Filters*

| Filter | Description |
| --- | --- |
| Group Name | The name of the group. Groups for which the sessions parameter is not a member of are listed. |
| Group Type | The type of group. Groups for which the sessions parameter is not a member of are listed. |
| Description | The description of the group. Groups for which the session parameter is not a member of are listed. |

3. Select the group or create a new group.

Figure 6–2 shows the dialog for adding a sessions parameter to an existing group.

*Figure 6–2    Add to Existing Group*



Figure 6–3 shows the dialog for creating a group to add a sessions parameter to.

*Figure 6–3   Create a New Group to Add Sessions Parameter to*



Enter the following information to create a group:

*Table 6–5    Add to Group Fields*

| Field | Description |
| --- | --- |
| Group Name | The name of the group. |
| Cache Policy | Groups offer two Cache Policy options: Full Cache or None. |
| | By default, the Cache Policy should be set to "all." |
| | For information, refer to **Cache Policy**. |
| Group Type | The type of group. |
| Description | Information about the group. |

When adding a group to an existing group, data from selected rows of the type the group can accept are added to the group. If any data is already in the group, an informational message is displayed. When creating a group to add the entity to, do not leave any fields blank; otherwise, an error occurs.

4.  Select **Open this group's detail tab when done**.

5.  Click **Add**.

    A confirmation dialog appears.

6.  Click **OK** to dismiss the confirmation dialog.

## 6.7  Session Details Page

The **Session Details** page consolidates information needed for fraud analysis.

To go to the **Session Details** page:

1.  In the **Search Results** table, click the **Session ID** of the session of interest. The **Session Details** page for that session is displayed.

General details and all of the actions performed during the session are captured in the Session Details page.

2.  View the details of the session.

## 6.8 Looking at Events from a Higher Level with Session Details

A **Session Details** page displays an overview of the events that transpired during a particular session for fraud analysis. It contains:

- General session data points such as user, device, location, and other details

- A forensic record of the session, including transactions and checkpoints that were evaluated. Each checkpoint displays the policies in that checkpoint, alerts that were triggered during the session for that checkpoint, and the final action for that checkpoint.

The policy explorer view is also available to provide additional details about policies, rules, and conditions.

### 6.8.1 Policy Explorer

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

*Figure 6–4   Policy Explorer*
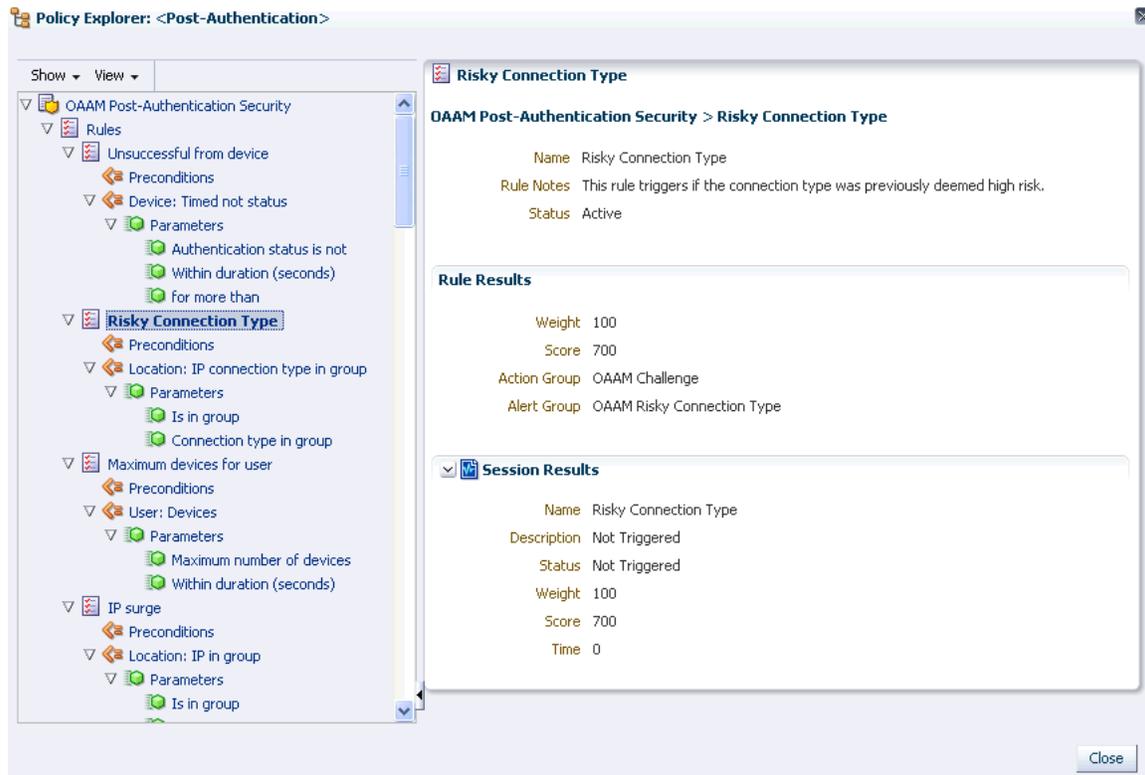


**Rule Details**

Details about the rule is shown in the Policy Explorer. The session results display the scores and results of that rule.

**Pre-conditions**

Pre-conditions for that rule is displayed in the details panel. The session results show the confidence factors and other values for the pre-conditions for that session.

**Conditions**

The values for the condition parameters are displayed. The session results show if the conditions returned true for this session evaluation.

**Trigger Combinations**

There is an option to view the triggered override combinations or view all overrides. Session results show the override information that was evaluated for this session including the nested policy information.

**Group Linking**

Group linking for the policy is displayed in the details panel.

## 6.8.2 Runtime Information

The **Session Details** page contains several panels. The main panels like checkpoints and transactions have multiple subpanels. Panel are not displayed if information is not available. Except for the **Session Details** panel, all other panels are displayed in the order of execution. (Looking at the Session Details page, you can see the flow of events, the sequence when the events happened within the session.)

*Figure 6–5   Session Details with Checkpoint, Alerts, Actions, and Policies*

### 6.8.2.1 Session Details

The **Session Details** panel shows all the related information regarding the login transaction. It shows the authentication status, IP address from which the user logged in, user name, User ID, cookie information, autolearning processing status, and the login time.

### 6.8.2.2 Policies

A list of policies in that checkpoint are displayed in the **Policies** panel. You can view the rules and action that triggered.

***Table 6–6 Policies in a Checkpoint***

| Item | Description |
|------|-------------|
| Name | The name of the policies that are under the checkpoint, rules under the policies, the conditions under the rules, and the action triggered. |
| Status | Executed (for policies) and Triggered (for rules). |
| Scoring Engine | A scoring engine is provided at the policy level and at the checkpoint level. |
| | The policy scoring engine is applied to rule scores to determine the risk for each policy. |
| Time | The time of the occurrence. |
| Weight | Percentage value used to influence the total score. |
| Score | Level of risk that has been calculated for specific situations or parts of a situation, expressed as a number. There are multiple policies under one checkpoint. The scores of these policies are used to determine a score for the checkpoint. |

As an investigator, you are interested in why a particular rule triggered. For example, you might look at which policy and rules triggered the alert.

Information can be gathered by looking at these details. For example, a user who successfully went through Pre-Authentication and Post-Authentication checkpoints knew the password and the questions and answers and there fore, there is a good chance that he is a valid user. On the other hand, a user who attempted to answer the questions twice and succeeded in providing a correct answer on his third attempt might be considered suspicious. This user did not know the answers right away so there is a chance that he may be a fraud trying out new answers.

To view more details about the policy, you can launch the Policy Explorer using the icon on top of the panel or from any of the icons within the table. The policy link displays the **Policy Details** page and the rules link displays the **Rule Details** page. Only active and triggered rules are displayed. Only active policies are displayed. You have the option to view all the rules in the Policy Explorer.

In the Policy Explorer, you can view the runtime values for each one of the policies and rules that were triggered. For example, if a rule triggered that showed that the user had logged in from a country that he did not usually log in from, you would want to look at the runtime details to see which country he logged in from. The Policy Explorer shows the policies that were triggered, the condition parameters, and the actual values.

### 6.8.2.3 Transactions

The Transactions panel displays a list of transactions that were created. You can view the actual transaction data and the entity attribute values used in the transactions. For example, a fraud investigator analyzing a session can see that a user was blocked performing a transaction and that a particular rule was triggered, and he can also see the amount that was passed in and the account number that was used in the transaction.

Transactions can be created within a checkpoint or without an associating checkpoint. If a Transaction ID is not provided (as in the case of a transaction without an associating checkpoint), OAAM processes the last transaction in the session. The

Transaction data for all transaction types are displayed in the Transactions panel of the session details page whether associated to a checkpoint or not. The Transaction checkpoints and policies are displayed in the order of execution along with other checkpoints, but the order of execution of the transactions and the checkpoints at which a particular transaction occurred cannot be determined.

### 6.8.3 Action, Alerts, and Scores

Table 6–6 shows an example of alerts, actions, and scores displayed in a Session Details page.

*Figure 6–6   Session Details: Alerts, Actions, and Scores*



#### Alerts

The Alerts panel shows alerts that were generated for a checkpoint during the session and details about the alerts, as shown in the table below. Each checkpoint could trigger multiple alerts. High-level alerts are displayed in bold red.

*Table 6–7   Sessions Checkpoint Actions*

| Item | Description |
| --- | --- |
| Level | Severity of the alert whether high, medium, low. |
| Alert Message | Text message configured in the alert. |
| Type | Type of the alert whether fraud, investigation, information, or other reason |
| Trigger Source | Rules that generated the particular alert |
| Timestamp | The time the alert was generated. |

#### Actions

All actions are displayed in the **Actions** panel with a Action Name column and a separate column indicating whether or not the action is final. The final action is also displayed in the top right section of checkpoint panel.

**Scores**

Scores are displayed for the policy and checkpoint. The scores are useful in detecting the probability of fraud or business scenarios and in decision making.

### 6.8.4 Outcomes from Each Checkpoints

Checkpoint panels are arranged in chronological order of execution and display the checkpoints and a list of the actions and alerts that were triggered at those checkpoints. By default, checkpoint panels are collapsed. In the initial opened view, only the transactions and the final alerts are displayed in the expanded form. All other subpanels are collapsed. You can expand all the panels to view additional information for that checkpoint.

The first checkpoint panel could be one for Pre-Authentication. On top of the panel, the total amount of time taken for this checkpoint to execute, the final action, and the final risk score are shown.

## 6.9 Investigation and the Importance of Details Pages

OAAM provides the capability to gather detailed information about the session parameters and to allow you to drill down further into the details involved in the session. For example, you need information to investigate logins so you perform a sessions search. From the results, you can see the country, location, and other session information, as shown in Figure 6–7.

*Figure 6–7   Sessions Search*



| Row | Session ID | Alerts | Organization ID | User Name | Device ID | IP Address | Location | Authentication Status | Login Time | Pre-Authentic Score | Pre-Authentic Action | Post-Auth Score | Post-Aut Action |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 548 | Medium Alerts: (1) | Default | test1111 | 206 | 192.0.2.253 | united states, californ | Pending | 4/14/2011 10:44 AM | 0 | Allow | 500 | Challeng |
| 2 | 547 | High Alerts: (1) | Default | paul | 403 | 198.51.100. | united states, californ | Blocked | 4/13/2011 2:54 PM | 0 | Allow | 700 | Challeng |
| 3 | 546 | High Alerts: (1) | Default | john | 402 | 198.51.100. | united states, californ | Blocked | 4/13/2011 2:52 PM | 0 | Allow | 700 | Challeng |
| 4 | 545 | High Alerts: (1) | Default | paresh | 402 | 198.51.100. | united states, californ | Blocked | 4/13/2011 2:52 PM | 0 | Allow | 700 | Challeng |
| 5 | 544 | Medium Alerts: (1) | Default | test1234 | 206 | 203.0.113.1 | united states, californ | Success | 4/13/2011 1:46 PM | 0 | Allow | 500 | Challeng |
| 6 | 543 | | Default | test1234 | 206 | 203.0.113.1 | united states, californ | Pending | 4/13/2011 1:43 PM | 0 | Allow | -1 | |
| 7 | 542 | Medium Alerts: (1) | Default | sr3 | 206 | 203.0.113.1 | united states, californ | Blocked | 4/13/2011 12:00 PM | 0 | Allow | 500 | Challeng |
| 8 | 541 | Medium Alerts: (1) | Default | sr3 | 206 | 203.0.113.1 | united states, californ | Success | 4/13/2011 11:58 AM | 0 | Allow | 500 | Challeng |
| 9 | 540 | | Default | mandar041401 | | 203.0.113.2 | Private, Private, Priva | Success | 4/13/2011 11:56 AM | 0 | Allow | 0 | Allow |
| 10 | 539 | | Default | mandar041401 | | 203.0.113.2 | Private, Private, Priva | Success | 4/13/2011 11:55 AM | 0 | Allow | 0 | Allow |
| 11 | 538 | | Default | mandar041401 | | 203.0.113.2 | Private, Private, Priva | Wrong Passw | 4/13/2011 11:55 AM | 0 | Allow | -1 | |
| 12 | 537 | Medium Alerts: (1) | Default | sr2 | 206 | 203.0.113.1 | united states, californ | Wrong Answ | 4/13/2011 11:51 AM | 0 | Allow | 500 | Challeng |

If you want to know more details about one of these, you can open a details page. These pages provide more information about the item you are interested in and allow you to filter out further and look at the related data to that particular item. In this example, if you open the location details page for the United States, you can look at the logins that only happened in the United States and all the devices used when users logged into the United States. Then, you can filter on the date created or updated if you want to look at the devices that were created during a particular time frame and used in logins from the United States. In this way, you are able to limit the data you wanted to view based on the detailed information you are looking at.

*Figure 6–8   Location Details (USA): Devices*



In fraud analysis an Investigator looks at sessions to find out more about what occurred. For example, to know if there was a pattern with a specific country or specific user, you would want to see more information about the user and country. For that, you would use the details pages. If you want to know if the United States belongs to a blacklist group or a monitor group, you can use the Groups tab of the Location Details page to search for those groups.

*Figure 6–9   Location Details (USA): Groups*



If you want to look at all the users who logged in from the United States, you can use the Users tab of the Location Details page to search on the authentication status for all the logins that were successful. You can also view the login failures from the country, the challenge success, and the challenge failure counts also.

*Figure 6–10   Location Details: Users*



You can also look at all the different alerts that were generated from the logins or sessions that occurred from the United States by using the Alerts tab of the Location Details page to search on the Alert ID, Alert Type, or Alert Level.

*Figure 6–11   Location Details: Alert*



## 6.10  Viewing Alerts

When an alert is generated it is associated with the user, device, and location that has taken part in the authentication. The login session holds information about the alert. Any changes to the alert type or alert message are automatically reflected in the alerts page. It shows the new information. Other than the Alerts tab, the detail pages display alert instances based on the level/type at the time they were triggered. Alert instances are grouped with the alert template they belong to. For example, if there were 10

sessions with alert level High last month and then the Administrator changed the level of that template to low, then the next 10 instances are displayed with the level Low.

## 6.11 User Details Page

The User Details page provides general details about the user and cross reference on other data types such as device, location, alerts, browser, OS, and so on. Also shown are details related to the user such as unique ID, Organization ID, groups the user belongs to, sessions and cache data, fingerprint, browser, OS, locale, and so on. You can open a User Details page to view details regarding that user by clicking the User Name or UserID link from the Sessions search, Session Details, and other pages.

Figure 6–12 shows a User Details page.

**Figure 6–12   User Details: Summary**
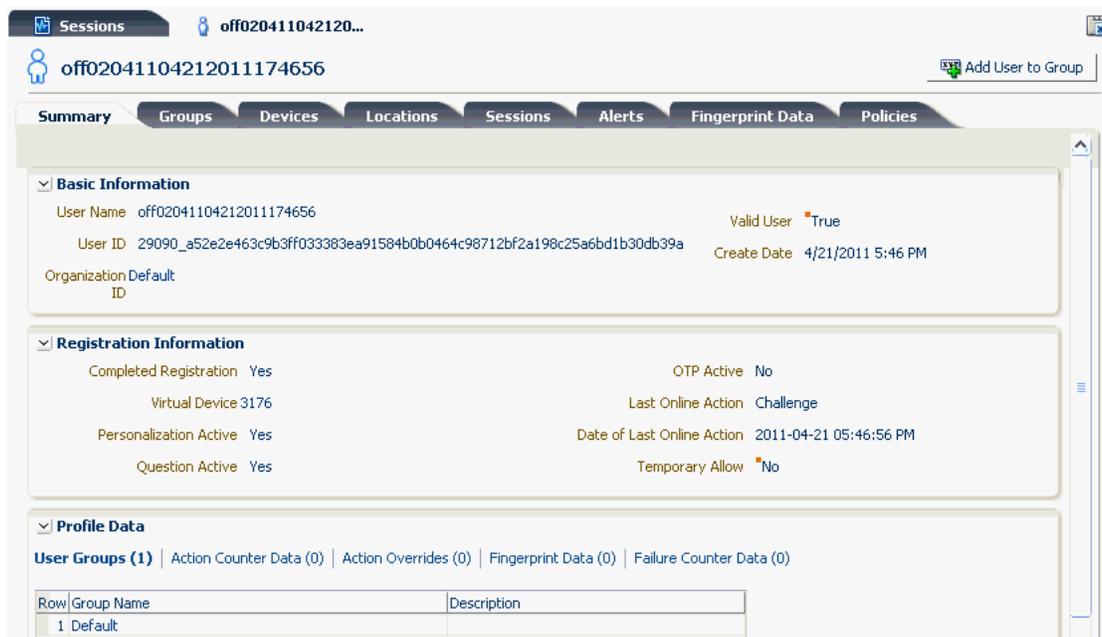


The User Details page is divided into the following tabs:

**Table 6–8   User Details Tabs**

| User Details Tab | Function |
| --- | --- |
| Summary | The Summary tab contains basic, registration, and profile information for the user. |
| Groups | The Groups tab shows a listing of the user groups that the user is a member of. |
| | The user can belong to User ID and User Name groups. |
| Locations | The Locations tab lists successful and unsuccessful login attempts from all user locations. This tab enables you to find out which locations and how many times a user logged in from a particular location. |
| Devices | The Devices tab lists all the devices that have been used in a session by the user during the time frame mentioned in the search criteria. It lists both successful and unsuccessful login attempts from all users' devices. This tab helps you find out which devices and how many times a device was used by the user. |

*Table 6–8   (Cont.)  User Details Tabs*

| User Details Tab | Function |
| --- | --- |
| Alerts | The Alerts tab lists alerts that are triggered and generated for a user by the application during the transaction process. The information shown is based on alert templates and not alert instances. Alert templates are displayed with the current details (level/type). |
| Sessions | The Sessions tab lists login sessions for a user for a particular period. |
| Policies | The Policies tab lists default and custom rules that are run for a user by the rules engine based on the checkpoints during authentication. |
| Fingerprint Details | The Fingerprint Details tab lists fingerprints created for the user during login. |

Detailed information about the User Details tabs follow.

## 6.11.1  User Details: Summary Tab

The Summary tab contains basic, registration, and profile information for the user.

### General Information

Table 6–9 summarizes the basic information about a user that is provided by the User Details: Summary Tab.

*Table 6–9     User Details: Basic Information about the User*

| Field | Definition |
| --- | --- |
| User Name | Login name given by user to login. |
| User ID | Unique Identifier of that device |
| Organization ID | Identifies the organization to which the user belongs. |
| Valid User | True if the user has authenticated successfully at least once. |
| Created Date | Date on which the user was created. Also, this refers to the first login date of the user. |

### Registration Information

The first time a user logs in, he must go through the registration process. Information is capture during the process. Table 6–10 summarizes the properties and attribute values that identify the status of each action performed by the user during the registration process.

*Table 6–10     User Details: Registration Information*

| Field | Definition |
| --- | --- |
| Completed Registration | (Yes/No) Identifies whether user has completed the registration process like registered challenge questions, image and phrase, which are unique for each user and used for identifying a user for security reasons. |
| Virtual Device Type | List of device IDs that the user registered as secure device during registration process. Maximum of three devices can be registered. |
| Personalization Active | (Yes/No) Identifies whether user registered Image and Phrase. |
| Question Active | (Yes/No) Identifies whether user registered Challenge Questions. |
| OTP Active | (Yes/No) Identifies whether user has been assigned One Time Password on SMS/Email Challenge. |

*Table 6–10 (Cont.) User Details: Registration Information*

| Field | Definition |
|---|---|
| Last Online Action | The last online action performed by user in his most recent transaction. |
| Date of Last Online Action | Date of last online action performed by user in his most recent transaction. |
| Temporary Allow | (Yes/No) Identifies whether the user was blocked and is allowed to access his account temporarily. |

### Profile Data

This Profile Data section lists important statistics about the user using cached data. Aggregate values are shown for User Groups, Action Counter Data, Action Override Data, Fingerprint Data, and Policies. These values use cache data and records are always shown even if the database is purged.

*Figure 6–13 Profile Data*
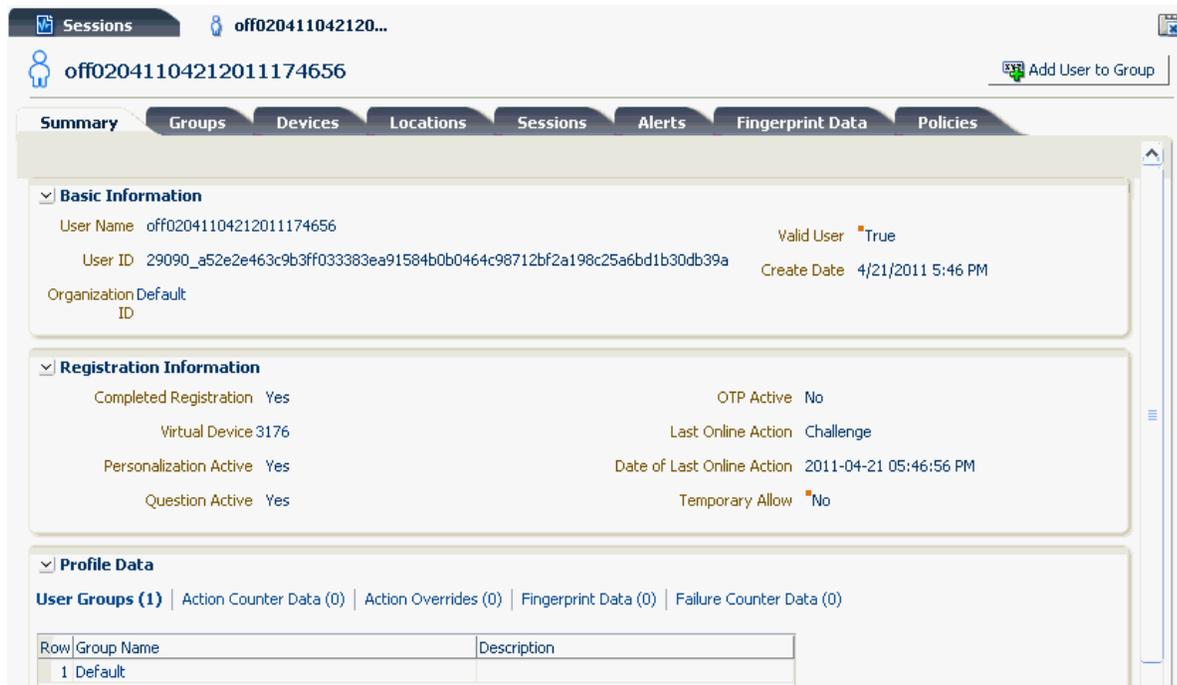


*Table 6–11 User Details; Profile Data*

| Field | Definition |
|---|---|
| User Groups | Lists groups associated with the user. |
| Action Counter Data | Lists the different actions performed by the user along with the aggregate count for each one of them. The data is available only if the "incrementCacheCounter" property is set to true in the "rule.action.enum". |

*Table 6–11  (Cont.)  User Details; Profile Data*

| Field | Definition |
| --- | --- |
| Action Overrides | Lists the checkpoints and the overriding actions for the user if an override is active like a temporary allow. |
| | For example, if the user was blocked earlier and is now allowed to access his account temporarily then, during Pre-authentication, instead of blocking the user, the user is allowed to proceed with the transaction (i.e. Block action is overridden to Allow). The values for overriding actions are configured in properties file. |
| Fingerprint Data | Lists the fingerprint information for the user if the cookies and flash are turned off. |
| | The Fingerprint Data ID numbers shown on this panel is the same as those shown in the fingerprint data tab. The difference between Fingerprint Data and the Fingerprint Data tab is that the tab shows the ID numbers and other information such as the browser, locale, and so on. |
| Failure Counter Data | List of Challenges faced by the user and total number of times the user failed to answer each one of them respectively. |

## 6.11.2  User Details: Groups Tab

The tab lists groups with which the user is associated. The user can belong to User ID and User Name groups.

*Figure 6–14  User Details: Groups*

The tab contains the following filter parameters.

*Table 6–12    User Details: Group Filters*

| Filters | Description |
| --- | --- |
| Group Name | Name of the group. You can enter the complete name or part of a group name. For example, if you enter new, any group with new in any part of its name is displayed. |
| Description | This filter maps to the User Group: description field |
| Cache Type | Groups offer two Cache Type options: Full Cache or None. For information, refer to **Cache Policy**. |
| Group Type | Category to which the group belongs. |

The search results show Group Name, Group Type, Cache Type, and Description columns. The default sorting is on Group Name. You can open the Group Details page by clicking the Group Name link.

### 6.11.3  User Details: Devices Tab

This tab lists all the devices that have been used in a session by the user during the time frame mentioned in the search criteria.

*Figure 6–15    User Details: Device Tab*
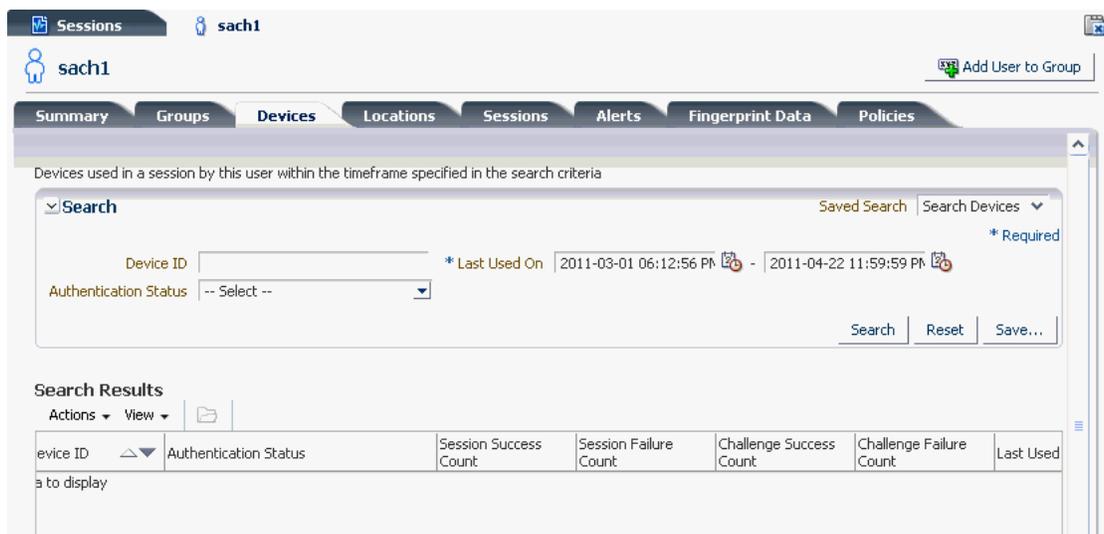


The tab contains the following filter parameters:

*Table 6–13    User Details: Device Tab*

| Field | Description |
| --- | --- |
| Device ID | Uniquely identifies each device and is autogenerated by the application. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the devices which were used by the user to login during the given time duration. |

Device ID, Authentication Status, Session Success Count, Session Failure Count, Challenge Success Count, Challenge Failure Count, and Last Used On information are shown. The default sorting is on the Device ID. Device ID is unique and hence a Device ID is not repeated more than once in the results.

The login/challenge success and failure counts correspond to the aggregate counts for the time frame.

You can open the Device Details page by clicking the Device ID link.

### 6.11.4 User Details: Locations Tab

This tab lists all the locations from where the user had made successful and unsuccessful login attempts.

*Figure 6–16   User Details: Locations*



The tab contains the following filter parameters:

*Table 6–14    User Details: Locations Tab*

| Filters | Description |
| --- | --- |
| Country | Country ID |
| State | State ID. The State list is dynamically populated with respect to what has been selected for Country. For example, if United States is selected, whatever states are available for that country are shown under States. |
| City | City ID. The City list is dynamically populated with respect to what has been selected for in Country and State. |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the locations from which the user logged in during the given time duration |

Results show the location, IP address, authentication status, session success count, session failure count, challenge success count, challenge failure count, and so on.

If a location is chosen in the search, the location may appear in the results as many times as the different IP addresses the user has used for the location. For each location there are associated success and failure counts.

Authentication Status and success and failure count values are related. For example, if there is a Success (1) value in the Authentication Status column, the Session Success Count column should show "1." If there is a Pending (1) value in the Authentication Status column, the Session Failure Count column should show "1."

Location on the result is always detailed to city level. For example, United States, California, Fremont. The default sorting is on the location name. Data cannot be edited on this page.

### 6.11.5 User Details: Sessions Tab

This tab lists login sessions for a user for a particular period.

**Figure 6–17   User Details: Sessions Tab**
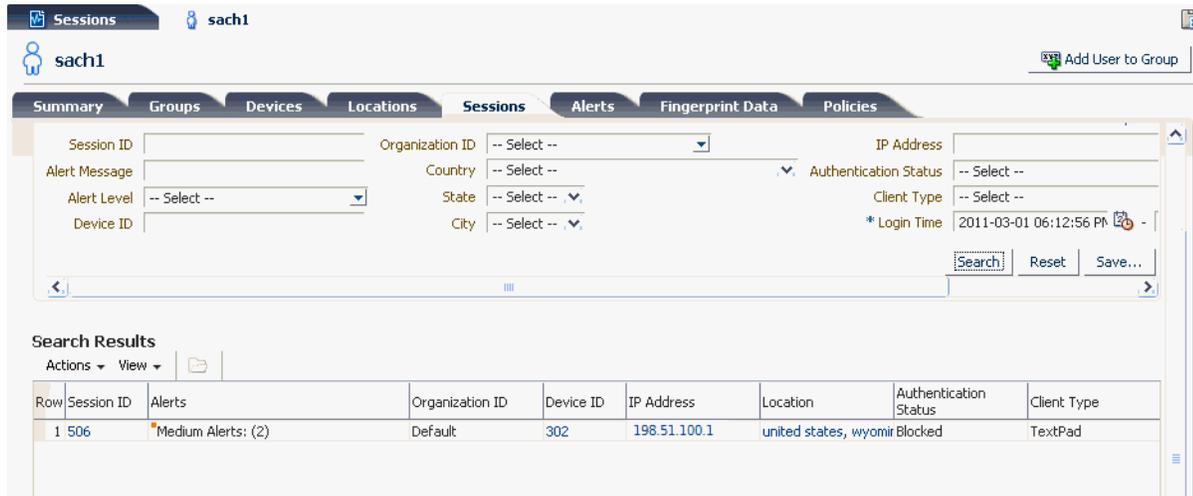


The tab contains the following filter parameters:

**Table 6–15    User Details: Sessions tab**

| Filter | Description |
|---|---|
| Session ID | Unique session identifier. |
| Alert Message | Display name describing the alert. Partial searches can be performed on alert messages. |
| Alert Level | Severity of the alert whether high, medium, low. |
| Device ID | Uniquely identifies each device and is autogenerated by the application. |
| Organization ID | Identifies the organization the user belongs to |
| Country | Country where the login or transaction occurred. |
| State | State where the login or transaction occurred. |
| City | City where the login or transaction occurred. |

*Table 6–15 (Cont.) User Details: Sessions tab*

| Filter | Description |
|---|---|
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Client Type | Virtual Authentication Devices. Device or application used for authentication or fingerprinting. For example: TextPad, KeyPad, Question Pad, login page, flash tracker. auth.client.type.enum is the enum used |
| Login time | Get all the sessions during which the device logged in for the given time duration. |

Session ID, Alerts, Organization ID, Device ID, IP Address, Location, Authentication Status, Client Type, Pre-Authentication Action, and Login Time shown.

## 6.11.6 User Details: Alerts Tab

This tab lists alerts that are triggered and generated for a user by OAAM Admin during transaction process. The information shown is based on alert templates and not alert instances. Alert templates are displayed with the current details (level/type).

The tab contains the following filter parameters:

*Table 6–16 User Details: Alert Filters*

| Filters | Description |
|---|---|
| Checkpoint | Decision and enforcement point when policies are call to run their rules. |
| | For information, refer to **Checkpoint**. |
| Policy Name | Name of the policy. The policy list is dynamically populated in respect to what has been selected for the checkpoint. |
| Rule Name | Rule that generated the alert. The rules list is dynamically populated in respect to what has been selected for the policy name. |
| Alert ID | ID of an alert. |
| Alert Message | Display name describing the alert. |
| Alert Level | Severity of the alert whether high, medium, low. |
| Alert Type | Type of the alert whether fraud, investigation, information, or other reason. |
| Session ID | Unique identifier for the session. |
| Date Triggered | Given time when the alerts triggered for the user. |

Figure 6–18 shows the Alerts tab of the User Details page.

*Figure 6–18   User Details: Alerts*
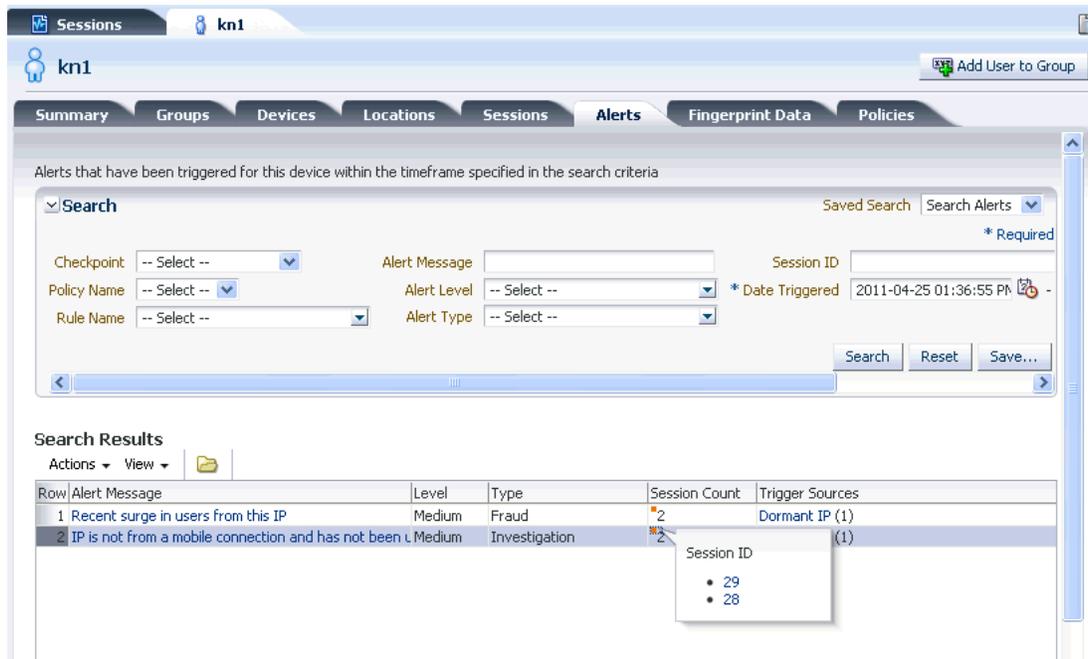


If you click an Alert Message link, details about the particular alert are shown. Details are shown for the level, alert types, and session count. In the example graphic above, the alert on the second row, "IP is not from a local mobile...," had generated in two sessions (shown in Session Count). If you click the Session Count link and then the session number, the Session Details page is displayed.

The trigger sources (name of rules) shows the rules that generated this particular alert and each one is associated with a count.

## 6.11.7  User Details: Fingerprint Data

This tab lists fingerprints created for the user during login. The tab contains the following filter parameters:

*Table 6–17   User Details: Fingerprint Data Tab*

| Filters | Description |
|---|---|
| Fingerprint ID | Unique ID generated for fingerprint by the application |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Browser Type | The type of browser a user is viewing pages with |
| OS Type | Type of operating system |
| Locale | A set of parameters that defines the user's language, country and any special variant preferences that the user wants to see in their user interface |
| Last Date Used | Get all the fingerprints created for the given time duration |

Information is captured on the devices the user used.

*Figure 6–19   User Details: Fingerprint Data*
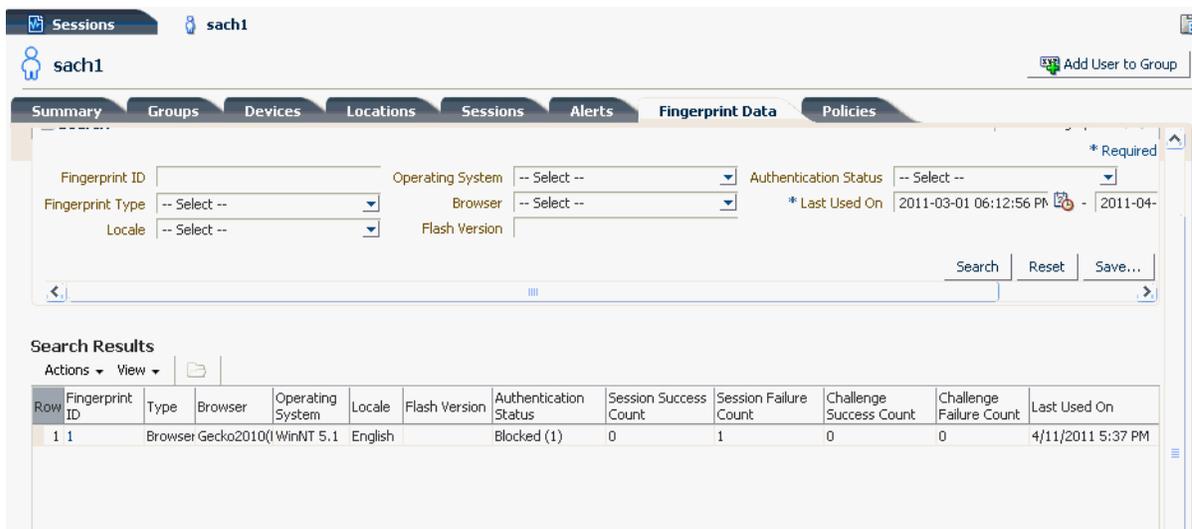


The Actions menu allows you to open the particular fingerprint.

*Figure 6–20   Fingerprint Details: Summary*
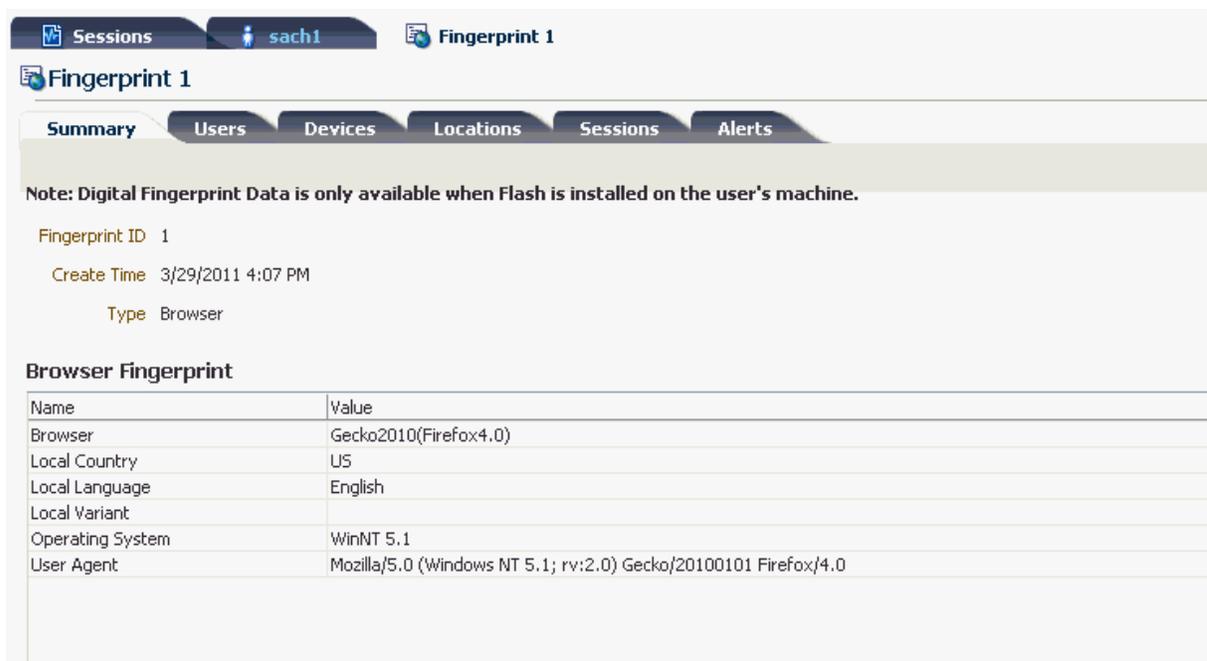


## 6.11.8  User Details: Policies Tab

This tab lists default and custom rules that are run for a user by the rule engine based on the checkpoints during authentication. The policies tab displays all the policies and rules that are run for the user including any nested policies in trigger combinations.

*Figure 6–21   User Details: Policies*



Only active policies and rules are displayed on this tab. If a policy is disabled it is not listed in this tab. Users can search for a specific checkpoint. The default sorting is on the name. The checkpoints is sorted alphabetically at the global level and the policies within each checkpoint is also sorted alphabetically.

## 6.11.9  User Details Tasks

This section describes how to obtain information about the user through the use of the User Details pages.

### 6.11.9.1  View general user information, registration information, and profile information

To view general user information, registration information, and profile information, click the User ID or User Name link from the sessions page for a valid user and view the Summary page.

### 6.11.9.2  View the actions performed by the user during registration

To view the actions performed by the user during registration:

1.  Click the User ID or User Name link from the Sessions page for a valid user.

    The User Details page is displayed.

2.  View the Registration Information section of the Summary tab for the status of each action performed by the user during the registration process.

### 6.11.9.3  View statistics about the user

To view statistics about the user:

1.  Click the User ID or User Name link from the Sessions page for a valid user.

    The User Details page is displayed.

2.  View the Profile Data / Cache Data section of the Summary tab.

### 6.11.9.4 Search and view the different devices used for a user to get additional information like the number of times a device is used by a user and the successful and unsuccessful login attempts from each device

To search and view the different devices used for a user to get additional information like the number of times a device is used by a user and the successful and unsuccessful login attempts from each device:

1. Click the User ID or User Name link from the Sessions page for a valid user.

   The User Details page is displayed.

2. Click the **Devices** tab.

3. Search for the different devices used for a user.

   This tab lists all the devices that have been used in a session by the user during the time frame mentioned in the search criteria

4. In the search results, view the following information for the devices for each user:

   - Login Failures

   - Login Successes

   - Challenge Failures

   - Challenge Successes

### 6.11.9.5 Search and view the different user groups with which a user is associated

To search and view the different user groups with which a user is associated:

1. Click the User ID or User Name link from the Sessions page for a valid user.

   The User Details page is displayed.

2. Click the **Groups** tab.

3. Search for the different groups with which the user is associated using the following parameters:

   A user can belong to User ID and User Name groups.

*Table 6–18   Group Filters*

| Filters | Description |
|---|---|
| Group Name | Name of the group. You can enter the complete name or part of a group name. For example, if you enter new, any group with new in any part of its name is displayed. |
| Group Type | Category to which the group belongs. |
| Cache Type | Groups offer two Cache Type options: Full Cache or None. <br> For information, refer to **Cache Policy**. |
| Group Description | This filter maps to the User Group: description field |

### 6.11.9.6 Search and view the different locations used for a user to get additional information such as the number of times a location is used by a user and the successful and unsuccessful login attempts from each location

To search and view the different locations used for a user to get additional information such as the number of times a location is used by a user and the successful and unsuccessful login attempts from each location:

1. Click the User ID or User Name link from the Sessions page for a valid user.

The User Details page is displayed.

2. Click the **Locations** tab.

3. Search for the different locations using the following filter parameters:

*Table 6–19    Location Tab*

| Filters | Description |
|---|---|
| Location | Country ID, State ID, City ID |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the locations from which the user logged in during the given time duration |

4. In the search results, view the following information for the device from each location:

   - Login Failures

   - Login Successes

   - Challenge Failures

   - Challenge Successes

### 6.11.9.7  Search and view all the alerts triggered and generated for the user

To search and view all the alerts triggered and generated for the user. The alerts are shown with different color codes to indicate the alert levels whether it is high, medium or low:

1. Click the User ID or User Name link from the Sessions page for a valid user.

   The User Details page is displayed.

2. Click the **Alerts** tab.

   This tab lists alerts that were triggered and generated for a user during the transaction process.

3. Search for the different alerts using the following filter parameters:

*Table 6–20    Alert Filters*

| Filters | Description |
|---|---|
| Alert Message | Display name describing the alert. |
| Alert ID | ID of an alert. |
| Alert Type | Type of this alert whether fraud, investigation, information, or other types. |
| Alert Level | Severity of the alert whether high, medium, low. |
| Rule Name | Rule that generated the alert. |
| Date Triggered | Given time when the alerts triggered for the user. |

4. In the search results, view the alerts triggered and generated for the user:

   The alerts are shown with different color codes to indicate the alert levels (whether is high, medium or low).

### 6.11.9.8 Search and view all the login sessions or search login sessions for a particular period for the user

To search and view all the alerts triggered and generated for the device. The alerts are shown with different color codes to indicate the alert levels whether it is high, medium or low:

1. Click the User ID or User Name link from the Sessions page for a valid user.

   The User Details page is displayed.

2. Click the **Sessions** tab.

   This tab lists login sessions for a user for a particular period.

3. Search for the different sessions using the following filter parameters:

*Table 6–21    Sessions tab*

| Filter | Description |
| --- | --- |
| Session ID | The unique identifier for a session. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Client Type | Virtual Authentication Devices. Device or application used for authentication or fingerprinting. For example: TextPad, KeyPad, Question Pad, login page, flash tracker. auth.client.type.enum is the enum used |
| Alert Level | Severity of the alert whether high, medium, low. |
| User Name | Login name given by user to login. |
| Organization ID | Identifies the organization to which the user belongs. |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Location | The place where the login or transaction occurred |
| Session Date | Get all the sessions during which the device logged in for the given time duration. |

### 6.11.9.9 View the rules run on the user

To view the rules run on the user:

1. Click the User ID or User Name link from the Sessions page for a valid user.

   The User Details page is displayed.

2. Click the **Policies** tab.

   This tab lists default and custom rules that are run for a user.

### 6.11.9.10 Search and view the fingerprints created for the user

To search and view the fingerprints created for the user:

1. Click the User ID or User Name link from the Sessions page for a valid user.

   The User Details page is displayed.

2. Click the **Fingerprints** tab.

   This tab lists fingerprints created for the user during login.

### 6.11.9.11  Add user to user group

You could add users to groups and create groups, using the **Add User to Group** button from search and details pages.

If you are viewing the details of a specific user, and based on the analysis, you identified this user as a fraudster, you could add this user to a blacklisted group from the dialog. You do not have to navigate away to the details page to add the user.

To add a user to a user group:

1. Click the User ID or User Name link from the Sessions page for a valid user.

   The User Details page is displayed.

2. Click **Add User To Group** at the upper right corner.

   The Add User to Group dialog is displayed.

3. Search for the group you want to add the user to by the group name.

   Only those groups that the user is not a member of are displayed.

4. Select the group to add the user to and click the **Add** button.

### 6.11.9.12  Create a new user group and add user to the newly created group

The Add User to Group and Add to Group dialogs allow you to search and view the details of a user group, before adding the user to that group. If you do not find the group to which this user belongs, a new group can be created.

If you perform a fraud analysis, and you identify that this particular user belongs to a certain group, but you do not have that group available, you can create that group. Then, you can add that particular user to that group.

To create a new user group and add user to the newly created group:

1. Click the User ID or User Name link from the Sessions page for a valid user.

   The User Details page is displayed.

2. Click the **Add User to Group** button at the upper right corner.

   The **Add to User** dialog is displayed.

3. Click **Create New Group** button and specify the details for the new group.

4. Select the **Open this Group's details tab when done** option.

5. Click the **Add** button.

   The group's details tab is displayed with the user added.

### 6.11.9.13  Remove user from user group

You can remove a user from the group from detail pages. For example, if you added a user to a monitor user group, and you have been monitoring the user for three months, and you realize that he or she is a valid user, you can remove that user from that group.

To remove a user from the user groups:

1. Click the User ID or User Name link from Sessions page for a valid user.

   The User Details page is displayed.

2. View the Groups tab.

   The Groups tab shows a listing of the groups.

3. Remove the user from a group by selecting a specific row and clicking the **Remove from group** button.

   You can select multiple rows to remove multiple users.

4. Click **Remove from Group**.

   The user is removed from the group selected.

   > **Note:** You should not be able to remove a user from the Organization ID of the primary user group.

### 6.11.9.14 Navigate to other details pages for groups, alerts, devices, locations, sessions, policy, rules and fingerprints

You can click a link from a tab to open the corresponding details pages.

- From the Users tab: click the User Name link to open the User Details page.

- From the Groups tab: click the Group Name link to open the Group Details page.

- From the Locations tab, click the Location or IP link to open the Location Details page.

- From the Alerts tab, click the Alert Message link to open the Alert Details page.

- From the Devices tab: click the Device ID link to open the Device Details page.

- From the Fingerprint tab: click the Fingerprint ID to open the corresponding fingerprint details page.

Links for User Name, IP address, session, and location are available on the Sessions tab.

## 6.12 IP or Locations (Country, State, or City) Details Page

IP, Country, State, or City Details pages provide details for an IP Address, country, state, or city, including mapping of city, state, country, cross reference on other data types such as device, user, alerts, sessions, browser, OS, locales, fingerprints, and so on.

You can drill down to the respective Location Details page by selecting either the IP Address, Country Name, State Name, or City Name shown in the Sessions search result or Case's sessions tab.

The Location Details page is divided into the following tabs:

*Table 6–22    Location Details Tabs*

| Location Details Tabs | Description |
| --- | --- |
| Summary | The Summary tab provides general location information. |
| Groups | The Groups tab lists groups which the location is associated to. |
| Users | The Users tab lists successful and unsuccessful login attempts by all users from the location. |
| Devices | The Devices tab lists successful and unsuccessful login attempts by all devices from the location. |

*Table 6–22   (Cont.)  Location Details Tabs*

| Location Details Tabs | Description |
| --- | --- |
| Alerts | The Alerts tab lists alerts that are generated for the location by the application during transaction process. |
| | The information shown is based on alert templates and not alert instances. |
| | Alert templates are displayed with the current details (level/type). |
| Sessions | The Sessions tab lists login sessions for a location for a particular period. |
| Fingerprints | The Fingerprints tab lists fingerprints created for the location during login. |

## 6.12.1  Location Details: Summary Tab

The Summary tab provides general location information. Information is displayed about country and state depending on the item selected. For example, if the user selected a city called "San Jose", the Summary tab displays the state and country name for that city. If the user selected the state called "California," only the country information is listed.

If you want to view IP Address details, you can click the IP Address link.

### Country Details

Table 6–23, " Country Details" lists the general country details that are displayed in the Summary tab of a Country Details page.

*Table 6–23    Country Details*

| Country Details | Description |
| --- | --- |
| Country ID | The ID of a country which is unique |
| Country Code | Geographical code (geocode) representing the country. |
| Country Name | Geographic name of country. |

### State Details

Table 6–24, " State Details" lists the general state details that are displayed in the Summary tab of a State Details page.

*Table 6–24    State Details*

| State Details | Description |
| --- | --- |
| State ID | The ID of a state. |
| State Code | Geographical code (geocode) representing the state. |
| State Name | Geographic name of state |
| Country Name | Geographic name of country the state belongs to. |

### City Details

Table 6–25, " City Details" lists the general city details that are displayed in the Summary tab of a City Details page.

*Table 6–25    City Details*

| City Details | Description |
| --- | --- |
| City ID | The ID of the city. |
| City Code | Geographical code (geocode) representing the city. |
| City Name | Geographic name of the city. |
| State Name | Geographic name of the state the city belongs to. |
| Country Name | Geographic name of the country the city belongs to. |

### IP Details

Table 6–26, " IP Details" lists the general IP information that are displayed in the Summary tab of the IP Details page.

*Table 6–26    IP Details*

| IP Details | Description |
| --- | --- |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| City Name | Geographic name of the city. |
| State Name | Geographic name of the state. |
| Country Name | Geographic name of the country. |
| Connection Speed | Internet connection speeds or bandwidths (high, medium, low). |
| Connection Type | Describes the data connection between the device or LAN and the internet. See the Connection Type mapping. |
| Routing Type | Tells how the user is routed to the internet. |
| Carrier | The name of the entity that manages the ASN entry. |
| ASN | Globally unique number assigned to a network or group of networks that is managed by a single entity. |
| Top-level Domain | The top-level domain of the URL. For example, .com in www.company.example.com. This is mapped through the Quova reference file. |
| Second-level Domain | The second-level domain of the URL. For example, Name in www.oracle.com. This is mapped through the Quova reference file. |
| City Confidence Factor | The confidence factor (1-99) that the correct city has been identified. |
| State Confidence Factor | The confidence factor (1-99) that the correct state has been identified. |
| Country Confidence Factor | The confidence factor (1-99) that the correct country has been identified. |

## 6.12.2  Location Details: Groups Tab

The Groups tab shows a listing of the geolocation groups the location belongs to.

Table 6–27, " Location Details: Group Filters" lists the filter parameters available for group searches.

*Table 6–27    Location Details: Group Filters*

| Filters | Description |
| --- | --- |
| Group Name | Name of the group. You can enter the complete name or part of a group name. For example, if you enter new, any group with new in any part of its name is displayed. |
| Group Description | This filter maps to the User Group: description field |
| Cache Type | Groups offer two Cache Type options: Full Cache or None. <br> For information, refer to **Cache Policy**. |

The group tab shows a listing of the groups which the location is associated to.

*Figure 6–22    Location Details (USA): Groups*
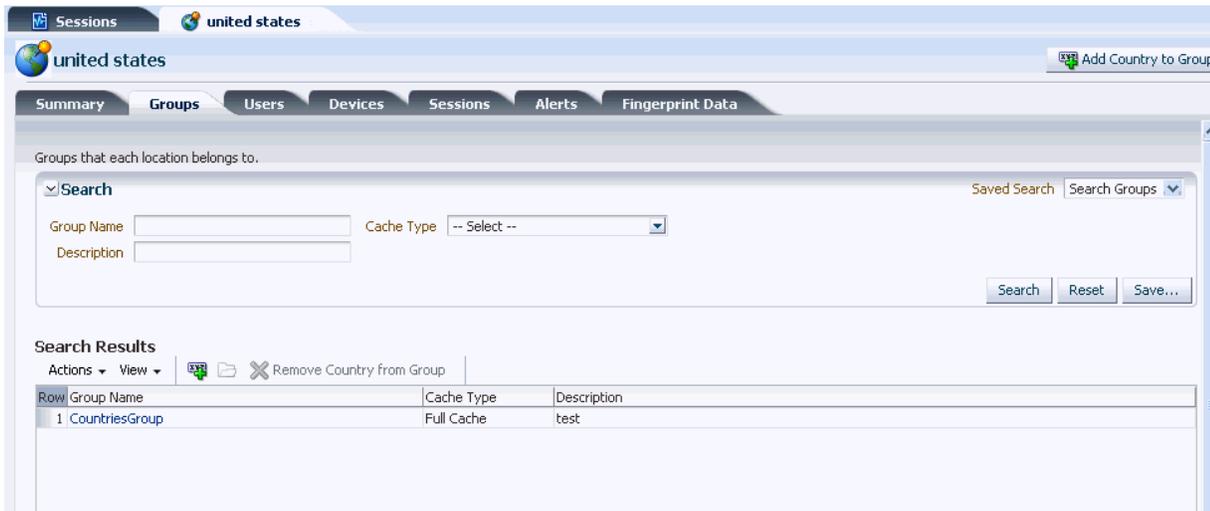


If the location belongs to multiple groups, all the groups are listed. Click the Group Name link to open the Group Details page. Click the IP Address link to view IP Address Details.

### 6.12.3  Location Details: Users Tab

This tab lists all the users who used the location during the time frame mentioned in the search criteria

Table 6–28, " Location Details: Users Tab" lists filter parameters available for user searches.

*Table 6–28    Location Details: Users Tab*

| Filter | Description |
| --- | --- |
| User Name | Login name given by user to login. |
| Organization ID | Identifies the organization to which the user belongs. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | The last date the location was used to log in. |

The search results display the User Name, Authentication Status, Last Used On, Login Failures, Login Successes, Challenge Failures, and Challenge Successes for each user.

*Figure 6–23    Location Details: Users*



By default, the results are displayed are sorted by User Name in ascending order. Only one row is displayed for each User Name. The login and challenge success and failure counts correspond to the aggregate counts for the time frame.

The user can open the User Details page by clicking the User Name link.

### 6.12.4  Location Details: Devices Tab

This tab lists all the devices used from the location during the time frame mentioned in the search criteria

Table 6–29, " Location Details: Device Tab" lists the filter parameters available for device searches.

*Table 6–29    Location Details: Device Tab*

| Field | Description |
| --- | --- |
| Device ID | Uniquely identifies each device and is autogenerated by the application. |
|  | No results are shown if you provide an invalid Device ID. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
|  | By default, the Authentication status is set to "all." |
|  | You can select multiple authentication status values. |
| Date Range | Get all the devices which were used by the user to login during the given time duration. |
|  | No results are shown if you provide an invalid date range. |

The search results display the Device ID, Authentication Status, Last Used On, Login Failures, Login Successes, Challenge Failures, and Challenge Successes for each user.

*Figure 6–24   Location Details (USA): Devices*



By default, the results are displayed are sorted by Device ID in ascending order. Only one row is displayed for each Device ID. The login and challenge success and failure counts correspond to the aggregate counts for the time frame.

A device details page can be opened by clicking the Device ID link.

## 6.12.5 Location Details: Alerts Tab

This tab lists all the alerts that have been triggered from the location during the date range provided. The information shown is based on alert templates and not alert instances. Alert templates are displayed with the current details (level/type).

The tab contains the following filter parameters.

*Table 6–30    Location Details: Alert Filters*

| Filters | Description |
|---------|-------------|
| Alert Message | Display name describing the alert. |
| Alert ID | ID of an alert. |
| Alert Type | Type of the alert whether fraud, investigation, information, or other types. Multiple alert types can be selected. |
| Alert Level | Severity of the alert whether high, medium, low. Multiple alert levels can be selected. |
| Rule Name | Rule that generated the alert. Multiple rules can be selected. |
| Date Triggered | Get all the alerts triggered during the given time duration for the user. |

The results display all the alert sources with the current details (level/type) for each alert message along with their count (total number of times the alert has been triggered).

*Figure 6–25   Location Details: Alert*



Clicking the Session ID in the search results opens the Sessions search page with pre-filled search parameters (Alert Level, Alert Message, Alert Type, Date, and so on).

## 6.12.6  Location Details: Sessions Tab

This tab lists login sessions for a location for a given time frame. It contains the following filter parameters:

*Table 6–31   Sessions tab*

| Filter | Description |
| --- | --- |
| Session ID | The unique identifier for a session. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Client Type | Virtual Authentication Devices. Device or application used for authentication or fingerprinting. For example: TextPad, KeyPad, Question Pad, login page, flash tracker. auth.client.type.enum is the enum used. |
| Alert Level | Severity of the alert whether high, medium, low. |
| Device ID | Uniquely identifies each device and is autogenerated by the application. |
| User Name | Login name given by user to login. |
| Organization ID | Identifies the organization to which the user belongs. |
| Session Date | The date the login or transaction occurred. |

By default the results are sorted by Session ID, which is unique. Clicking the Device ID, IP address, User Name, or alerts link opens the corresponding details page.

## 6.12.7  Location Details: Fingerprints Tab

This tab lists fingerprints created for the location during login.

*Figure 6–26   Location Details: Fingerprint Data*



The tab contains the following filter parameters:

*Table 6–32    Fingerprint Data*

| Filters | Description |
| --- | --- |
| Fingerprint ID | Unique ID generated for fingerprint by the application |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Browser Type | The type of browser a user is viewing pages with |
| OS Type | Type of operating system |
| Locale | A set of parameters that defines the user's language, country and any special variant preferences that the user wants to see in their user interface |
| Last Date Used | Get all the fingerprints created for the given time duration |

By default, the results are sorted by browser Fingerprint ID. The browser/flash fingerprint combination is unique and hence each combination has only one row in the results table. The Fingerprint ID has a link and opens the corresponding Fingerprint Details page.

### 6.12.8  Location (Country, State, City, or IP) Details Tasks

This section describes how to obtain information through the use of the Location Details pages.

#### 6.12.8.1  View general information about the location

To view general information about a location:

1.  From the results of a session search, click the country, state, city, or IP link.

    The Location Details page for that country, state, city, or IP is displayed.

2.  View the Summary tab.

On the Summary tab, additional information is displayed about the country and state depending on the item selected.

For example, if you select a city called "San Jose," the Summary tab displays the state and country names for that city. If you select the state "California," only the country information is listed.

For details on the information displayed on the Summary tab, refer to Section 6.12.1, "Location Details: Summary Tab."

### 6.12.8.2 Search and view the different location groups to which a location is associated or belongs

To search and view the different location groups that a location is associated with or belongs to:

1.  From the results of a session search, click the country, state, city, or IP link.

    The Location Details page for that country, state, city, or IP is displayed.

2.  Click the **Groups** tab.

3.  Search and view the different location groups to which a location is associated or belongs by using the following filters:

*Table 6–33    Location Details: Group Filters*

| Filters | Description |
| --- | --- |
| Group Name | Name of the group. You can enter the complete name or part of a group name. For example, if you enter new, any group with new in any part of its name is displayed. Group Name is not case sensitive. |
|  | No records are shown if you enter an invalid Group Name. |
| Cache Type | Groups offer two Cache Type options: Full Cache or None. |
|  | By default, the Cache Type should be set to "all." |
|  | For information, refer to **Cache Policy**. |
| Group Description | The description for the group. |
|  | Group Description is case insensitive. You can enter part of the group description. |
|  | No results are shown if you enter special characters or a description that is too long. |

The group tab shows a listing of the geolocation groups the location belongs to. If the location belongs to multiple groups, all the groups are listed. You can open the Group Details page by clicking the Group ID link.

### 6.12.8.3 Add location to existing location group

Only Security Administrators, System Administrators, and Investigators have access to the **Add to Group** command. CSRs do not have access to the **Add to Group** command. The **Add to Group** button is available in the Sessions search and other details pages.

Locations can be added to geolocation group types. A location can be added to only one location group at a time.

To add a location to a location group:

1.  In the Sessions search or other details page, click the location link.

    The Location Details page is displayed.

2.  Click the **Add Location to Group** button at the upper right corner.

The **Add to Group** dialog is displayed.

3. Search for the group you want to add the location to by the group name.

   Only those groups that the location is not a member of are displayed.

   If you do not find the country, state, or city group you need, you can create a new group. Information for doing so is provided later.

4. Select the group to add the location to and the **Open this Group's details tab when done** option.

5. Click the **Add** button.

   The group's details tab is displayed with the location added.

### 6.12.8.4  Create a location group and add location to it

To create a location group and add the location to it:

1. In the Sessions search or other details page, click the location link.

   The Location Details page is displayed.

2. Click the **Add Location to Group** button at the upper right corner.

   The **Add to Group** dialog is displayed.

3. Click **Create New Group** button and specify the details for the new group.

4. Select the **Open this Group's details tab when done** option.

5. Click the **Add** button.

   The group's details tab is displayed with the location added.

### 6.12.8.5  Search and view the different users that logged in from the location get additional information like the number of times a user logged in from the location and the successful and unsuccessful login attempts from the location by each user

To search and view the different users that logged in from the location get additional information like the number of times a user logged in from the location and the successful and unsuccessful login attempts from the location by each user:

1. From the results of a session search, click the country, state, city, or IP link.

   The Location Details page for that country, state, city, or IP is displayed.

2. Click the **Users** tab.

   - To see additional information such as the number of times a user logged in from the location, search by User Name. The Login Successes column displays the number of times a user logged in.

   - To see the number of successful and unsuccessful login attempts from the location by each user, select **Blocked** and **Success** as the Authentication Status.

     Login failures and successes are displayed for each user.

### 6.12.8.6  Search and view the different devices that logged in from the location get additional information like the number of times a device logged in from the location

**and the successful and unsuccessful login attempts from the location by each device**

To search and view the different devices that logged in from the location get additional information like the number of times a device logged in from the location and the successful and unsuccessful login attempts from the location by each device:

1. From the results of a session search, click the country, state, city, or IP link.

   The Location Details page for that country, state, city, or IP is displayed.

2. Click the **Devices** tab.

   - To see additional information such as the number of times a device was used to log in from the location, search by Device ID. The Login Successes column displays the number of times a device was used to log in.

   - To see the number of successful and unsuccessful login attempts from the location by each device, select **Blocked** and **Success** as the Authentication Status.

     Login failures and successes are displayed for each device.

### 6.12.8.7 Search and view all the alerts triggered and generated for the location

To search and view all the alerts triggered and generated for the location. The alerts are shown with different color codes to indicate the alert levels whether it is high, medium or low

1. From the results of a session search, click the country, state, city, or IP link.

   The Location Details page for that country, state, city, or IP is displayed.

2. Click the **Alerts** tab and view the results table for the alert levels.

### 6.12.8.8 Search and view all the login sessions or search login sessions for a particular period for the location

To search and view all the login sessions or search login sessions for a particular period for the location:

1. From the results of a session search, click the country, state, city, or IP link.

   The Location Details page for that country, state, city, or IP is displayed.

2. Click the **Sessions** tab.

3. Enter session dates to get sessions for that period for the location.

### 6.12.8.9 Search and view the fingerprints created for the location

To search and view the fingerprints created for the location:

1. From the results of a session search, click the country, state, city, or IP link.

   The Location Details page for that country, state, city, or IP is displayed.

2. Click the **Fingerprint Data** tab.

3. Search by OS, locale, browser, Fingerprint ID, and so on.

### 6.12.8.10 Navigate to other details pages for groups, alerts, devices, users, sessions and fingerprints

You can click the links in tabs to open the corresponding details page:

- From the Summary tab: click the IP Address link to view IP Address Details.

- From the Groups tab: click the Group Name link to open the Group Details page.

- From the Devices tab: click the Device ID link to open the Device Details page.

- From the Users tab: click the User Name link to open the User Details page.

- From the Alerts tab: click the Session ID to open the Sessions search page with pre-filled search parameters (Alert Level, Alert Message, Alert Type, Date, and so on

- From the Fingerprint tab: click the Fingerprint ID to open the corresponding Fingerprint Details page.

On the Sessions tab, links are provided for the following pages

- For the Session Details - Links are provided for session ID

- For IP Details - Links are provided for Country, State and City

- For Country Details - Links are provided for IP, State and City

- For State Details - Links are provided for IP, Country and City

- For City Details - Links are provided for IP, Country and State

## 6.13 Device Details Page

The Device Details page displays details about a device including cross reference on other data types such as user, location, alerts, browser, sessions, full list of fingerprint data, and so on. You can open the Device Details page by clicking any Device ID link from the Sessions search, Session Details, or other listing pages.

The Device Details page is divided into the following tabs:

*Table 6–34    Device Details Tabs*

| Device Details Tabs | Descriptions |
| --- | --- |
| Summary | The Summary tab provides general device information. |
| Groups | The Groups tab list groups with which the device is associated. For example Restricted Devices Group. |
| Users | The Users tab lists successful and unsuccessful login attempts from all users using the device. This report helps to find out which users and how many times a user used the device for login. |
| Locations | The Locations tab lists successful and unsuccessful login attempts from all devices' locations. This report helps to find out which locations and how many times a device logged in from a particular location. |
| Sessions | The Sessions tab lists login sessions for a device for a particular period. |
| Alerts | The Alerts tab lists alerts that are triggered and generated for a device by OAAM Admin during transaction process. The information shown is based on alert templates and not alert instances. Alert templates are displayed with the current details (level/type). |
| Fingerprint Data | The Fingerprint tab shows browser and flash fingerprint information for the device. |
| Fingerprint Details | The Fingerprint Details tab lists fingerprints created for the device during login. |

### 6.13.1 Device Details: Summary Tab

The Summary tab provides general device information. The following information is provided:

**Basic Information**

*Table 6–35    Device Details Basic Information*

| Device Details Summary Tab | Description |
|---|---|
| Device ID | Uniquely identifies each device and is autogenerated by the application. |
| Operating System | Device OS. The information is fetched from the fingerprint data associated with the device |
| Browser | Device Browser type. The information is fetched from the fingerprint data associated with the device |
| Create Date | Date on which the user has first used the device for authentication. Also, this refers to the first login date of the device. |
| Last Used On | This date refers to the most recent login time from the device. |

**Fingerprinting Information**

*Table 6–36    Device Details Fingerprint Information*

| Device Details Fingerprint Tab | Description |
|---|---|
| Browser Fingerprint Data | This field shows information such OS type, browser type, and so on. |
| Flash Fingerprint Data | This field shows information such as OS type, browser type, Player Type, Has audio, Has mp3, Supports streaming audio, and so on. |

### 6.13.2 Device Details: Groups Tab

This tab lists groups to which the device is associated. For example, Restricted Devices. The tab contains the following filter parameters:

*Table 6–37    Device Details: Group Filters*

| Filters | Description |
|---|---|
| Group Name | Name of the group. You can enter the complete name or part of a group name. For example, if you enter new, any group with new in any part of its name is displayed. |
| Description | This filter maps to the User Group: description field |
| Cache Type | Groups offer two Cache Type options: Full Cache or None. For information, refer to **Cache Policy**. |

You can open the Group Details page by clicking the Group ID link.

### 6.13.3 Device Details: Users Tab

This tab lists successful and unsuccessful login attempts from all users using the device. The tab contains the following filter parameters.

*Table 6–38    Device Details: User tab*

| Filter | Description |
|---|---|
| User Name | Login name given by user to login. |
| Organization ID | Identifies the organization to which the user belongs. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the users who used the device to login during the given time duration. |

The results are sorted by User Name and in ascending order. Each user is displayed only once in the results. You can open the User Details by clicking the User ID link

### 6.13.4  Device Details: Locations Tabs

This tab lists successful and unsuccessful login attempts from all locations. The tab contains the following filter parameters.

*Table 6–39    Device Details: Location Tab*

| Filters | Description |
|---|---|
| Location | Country ID, State ID, City ID |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the locations from which the user logged in during the given time duration |

The Locations are displayed multiple times, if the IP is different for the same device used to log in from the same location. Location is sorted by name and in ascending order. The login/challenge success and failure counts correspond to the aggregate counts for the time frame.

You can open the IP Details page by clicking the IP address link.

### 6.13.5  Device Details: Alerts Tab

This tab lists alerts that are generated for a device during transaction process. The information shown is based on alert templates and not alert instances. Alert templates are displayed with the current details (level/type).

The tab contains the following filter parameters.

*Table 6–40    Device Details: Alert Filters*

| Filters | Description |
|---|---|
| Checkpoint | Decision and enforcement point when the policies were called to run their rules |
| Policy Name | The name of the policy. The policy list is dynamically populated in respect to what has been selected for the checkpoint. |
| Rule Name | Rule that generated the alert. |
| Alert Message | Display name describing the alert. |
| Alert ID | ID of an alert. |
| Alert Level | Severity of the alert whether high, medium, low. |

*Table 6–40   (Cont.)  Device Details: Alert Filters*

| Filters | Description |
| --- | --- |
| Alert Type | Type of the alert whether fraud, investigation, information, or other types. |
| Session ID | The ID of the session |
| Date Triggered | Given time when the alerts triggered for the user. |

The results displays all the alert sources for each alert message along with their count (total number of times it has been triggered).

By default the results are sorted by alert messages in ascending order.

Clicking the Session ID opens the Sessions search page with pre-filled search parameters (Alert Level, Alert Message, Alert Type and Date).

## 6.13.6  Device Details: Sessions Tab

This tab lists login sessions for a device for a particular period. The tab contains the following filter parameters.

*Table 6–41     Sessions tab*

| Filter | Description |
| --- | --- |
| Session ID | The unique identifier for the session. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Client Type | Virtual Authentication Devices. Device or application used for authentication or fingerprinting. For example: TextPad, KeyPad, Question Pad, login page, flash tracker. auth.client.type.enum is the enum used |
| Alert Level | Severity of the alert whether high, medium, low. |
| User Name | Login name given by user to login. |
| Organization ID | Identifies the organization to which the user belongs. |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Location | The geolocation. |
| Session Date | Get all the sessions during which the device logged in for the given time duration. |

By default, the results are sorted by Session ID in descending order.

Session ID is usually unique unless the IP or device has changed while the session is in progress.

## 6.13.7  Device Details: Fingerprint Data Tab

This tab lists fingerprints created for the device during login.

*Figure 6–27   Device Details: Fingerprint Data*



The tab contains the following filter parameters.

*Table 6–42    Device Details: Fingerprint Data*

| Filters | Description |
|---|---|
| Fingerprint ID | Unique ID generated for fingerprint by the application |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Browser Type | The type of browser a user is viewing pages with |
| OS Type | Type of operating system |
| Locale | A set of parameters that defines the user's language, country and any special variant preferences that the user wants to see in their user interface |
| Last Date Used | Get all the fingerprints created for the given time duration |

## 6.13.8  Device Details Tasks

This section describes how to obtain information through the use of the Device Details pages.

### 6.13.8.1  View general information about the device

To view general information about the device:

1.  Click the Device ID link in the Session search page or other pages.

    The Device Details page is opened and shows additional details.

2.  View the Summary tab.

    The following general data is displayed:

    -   Device ID

    -   OS

    -   Browser

    -   Created Date

    -   Last Used On

### 6.13.8.2 View flash and browser fingerprint information created for the device

To view general information about the device:

1. Click the Device ID link in the Session search page or other pages.

   The Device Details page is opened and shows additional details.

2. View the Fingerprint Data tab.

   Flash and Browser Fingerprint data is shown.

### 6.13.8.3 Search and view the different device groups to which a device is associated or belongs

To search and view the different device groups to which a device is associated or belongs:

1. Click the Device ID link in the Session search page or other pages.

   The Device Details page is opened and shows additional details.

2. View the Groups tab.

3. Search groups using the following filters:

*Table 6–43    Group Filters*

| Filters | Description |
| --- | --- |
| Group Name | Name of the group. You can enter the complete name or part of a group name. For example, if you enter new, any group with new in any part of its name is displayed. |
| Group Type | Category to which the group belongs. |
| Cache Type | Groups offer two Cache Type options: Full Cache or None. |
|  | For information, refer to **Cache Policy**. |
| Group Description | This filter maps to the User Group: description field |

### 6.13.8.4 Add/Remove Device from a Device Group

To add a device to a device group:

1. In the Sessions search or other details page, click the Device ID link.

   The Device Details page is displayed.

2. Click the **Add Device to Group** button at the upper right corner.

   The **Add to Group** dialog is displayed.

3. Search for the group you want to add the device to by the group name and device group type.

   Only those groups that the device is not a member of are displayed.

   If you do not find the device group you need, you can create a new group. Information for doing so is provided later.

4. Select the group to add the device to and the **Open this Group's details tab when done** option.

5. Click the **Add** button.

   The group's details tab is displayed with the device added.

To remove a device from a device group:

1. Click the Device ID link in the Session search page.

   The Device Details page is opened and shows additional details.

2. View the Groups tab.

   The Groups tab shows a listing of the groups. The device is a member of all these device groups.

3. Click the Device Group that contains the device.

4. In the details page of the group, click the Devices tab.

5. Remove the device from a group by selecting the specific row and clicking the **Delete selected members** button on the toolbar.

6. Click **Delete** on the **Confirmation** dialog.

7. Click **OK** to dismiss the **Information** dialog.

   The device is removed from the group selected.

### 6.13.8.5 Create a device group and add device to it

To create a device group and add the device to it:

1. In the Sessions search or other details page, click the Device ID link.

   The Device Details page is displayed.

2. Click the **Add Device to Group** button at the upper right corner.

   The **Add to Group** dialog is displayed.

3. Click **Create New Group** button and specify the details for the new group.

4. Select the **Open this Group's details tab when done** option.

5. Click the **Add** button.

   The group's details tab is displayed with the device added.

### 6.13.8.6 Search and view the different users that used the device to login to get additional information like the number of times the device was used by a user and the successful and unsuccessful login attempts for the device by each user

To search and view the different users that used the device to login to get additional information like the number of times the device was used by a user and the successful and unsuccessful login attempts for the device by each user:

1. Click the Device ID link in the Session search page or other pages.

   The Device Details page is opened and shows additional details.

2. Click the **Users** tab.

3. Search for the different users using the following filter parameters:

*Table 6–44    User tab*

| Filter | Description |
| --- | --- |
| User Name | Login name given by user to login. |

*Table 6–44 (Cont.) User tab*

| Filter | Description |
| --- | --- |
| Organization ID | Identifies the organization to which the user belongs. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the users who used the device to login during the given time duration. |

4. In the search results, view the following:

- Failure Counter (the login fail count)

- Success Counter (the login success count)

### 6.13.8.7 Search and view the different locations from which the device was used for login to get additional information like the number of times the device was used from a location and the successful and unsuccessful login attempts for the device from each location

To search and view the different locations from which the device was used for login to get additional information like the number of times the device was used from a location and the successful and unsuccessful login attempts for the device from each location:

1. Click the Device ID link in the Session search page or other pages.

   The Device Details page is opened and shows additional details.

2. Click the **Locations** tab.

3. Search for the different locations using the following filter parameters:

*Table 6–45 Location Tab*

| Filters | Description |
| --- | --- |
| Location | Country ID, State ID, City ID |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the locations from which the user logged in during the given time duration |

4. In the search results, view the following for the device from each location:

- Failure Counter (the login fail count)

- Success Counter (the login success count)

### 6.13.8.8 Search and view all the alerts triggered and generated for the device

To search and view all the alerts triggered and generated for the device. The alerts are shown with different color codes to indicate the alert levels whether it is high, medium or low:

1. Click the Device ID link in the Session search page or other pages.

   The Device Details page is opened and shows additional details.

2. Click the **Alerts** tab.

This tab lists alerts that are triggered and generated for a device during transaction process.

3. Search for the different alerts using the following filter parameters:

*Table 6–46    Alert Filters*

| Filters | Description |
| --- | --- |
| Alert Message | Display name describing the alert. |
| Alert ID | ID of an alert. |
| Alert Type | Type of the alert whether fraud, investigation, information, or other types. |
| Alert Level | Severity of the alert whether high, medium, low. |
| Rule Name | Rule that generated the alert. |
| Date Triggered | Given time when the alerts triggered for the user. |

4. In the search results, view the alerts triggered and generated for the device:

The alerts are shown with different color codes to indicate the alert levels (whether is high, medium or low).

### 6.13.8.9  Search and view all the login sessions or search login sessions for a particular period for the device

To search and view all the alerts triggered and generated for the device. The alerts are shown with different color codes to indicate the alert levels whether it is high, medium or low:

1. Click the Device ID link in the Session search page or other pages.

The Device Details page is opened and shows additional details.

2. Click the **Sessions** tab.

This tab lists login sessions for a device for a particular period.

3. Search for the different sessions using the following filter parameters:

*Table 6–47    Sessions tab*

| Filter | Description |
| --- | --- |
| Session ID | The unique identifier for a session. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Client Type | Virtual Authentication Devices. Device or application used for authentication or fingerprinting. For example: TextPad, KeyPad, Question Pad, login page, flash tracker. auth.client.type.enum is the enum used |
| Alert Level | Severity of the alert whether high, medium, low. |
| User Name | Login name given by user to login. |
| Organization ID | Identifies the organization to which the user belongs. |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Location | Place where login or transaction occurred |
| Session Date | Get all the sessions during which the device logged in for the given time duration. |

### 6.13.8.10 Search and view the fingerprints created for the device

To search and view the fingerprints created for the device:

1. Click the Device ID link in the Session search page or other pages.

   The Device Details page is opened and shows additional details.

2. Click the **Fingerprint Data** tab.

   This tab lists the fingerprints created for the device during login.

### 6.13.8.11 Navigate to other details pages for groups, alerts, users, locations, sessions and fingerprints

You can click links on a tab in a details page to open other details pages:

- From the Users tab: click the User Name link to open the User Details page.

- From the Groups tab: click the Group Name link to open the Group Details page.

- From the Locations tab, click the Location link to open the Location Details page.

- From the Alerts tab: click the Alert Message to open the Alert Details page.

- Links for User Name, IP address, session, and location are available on the Sessions tab.

## 6.14 Browser or Flash Fingerprint Details

You can drill down to the Fingerprint Details page from the Sessions search results by selecting a Browser or Flash Fingerprint ID.

There are two different kinds of Fingerprint Details pages:

- Flash Fingerprint

- Browser Fingerprint

### 6.14.1 Fingerprint Details: Summary Tab

The Fingerprint Details Summary page shows general fingerprint information and the data collected during device fingerprinting.

*Figure 6–28   Fingerprint Details: Summary*
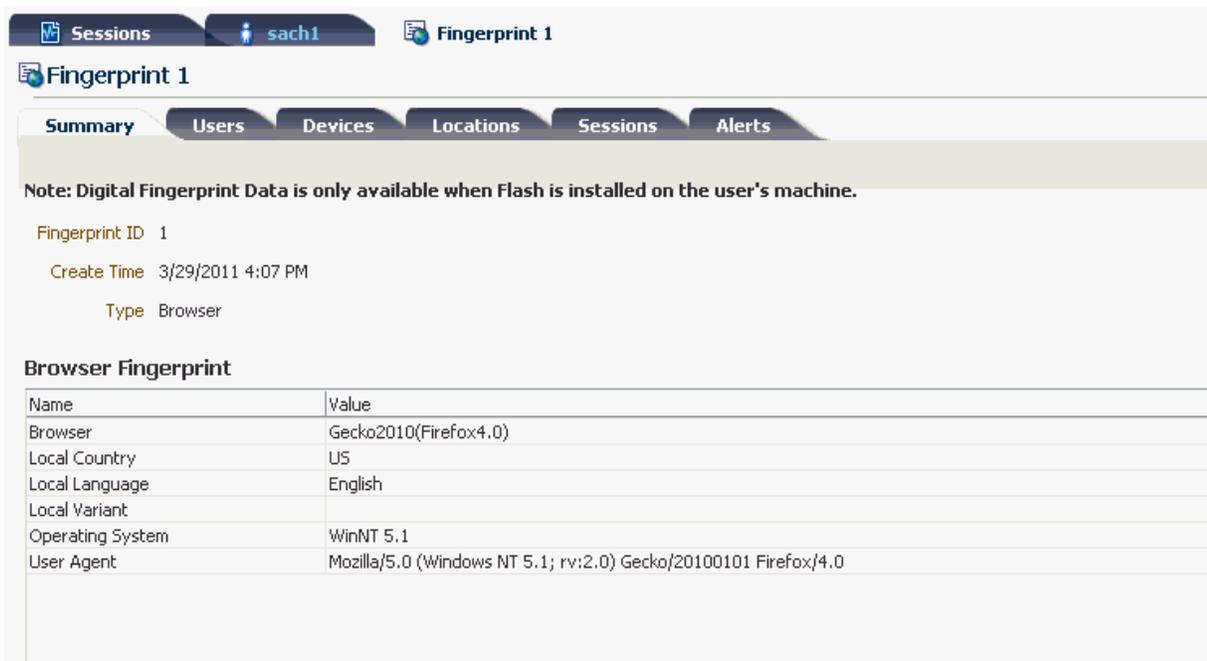


The basic information provided by this tab include:

*Table 6–48    Fingerprint Details Tab*

| Fingerprint Details | Description |
| --- | --- |
| Fingerprint ID | Unique ID generated for fingerprint by the application |
| Fingerprint Type | Type of fingerprint, whether the fingerprint is a flash or browser fingerprint. |
| Created Date | Date on which the fingerprint was created in the system |

Depending on the Fingerprint type, Fingerprint data provided by this tab may include browser, OS, locale information and digital information such as Player Type, Has audio, Has mp3, Supports streaming audio, and so on. Flash fingerprint information is available only if flash is installed on the user-client's machine.

## 6.14.2  Fingerprint Details: Users Tab

This tab lists all the users who used the fingerprint during the time frame specified. The Users tab of the Fingerprint Details page enables you to determine which users and how many times the fingerprint was used for each user during the login process.

*Figure 6–29   Fingerprint Details: User*
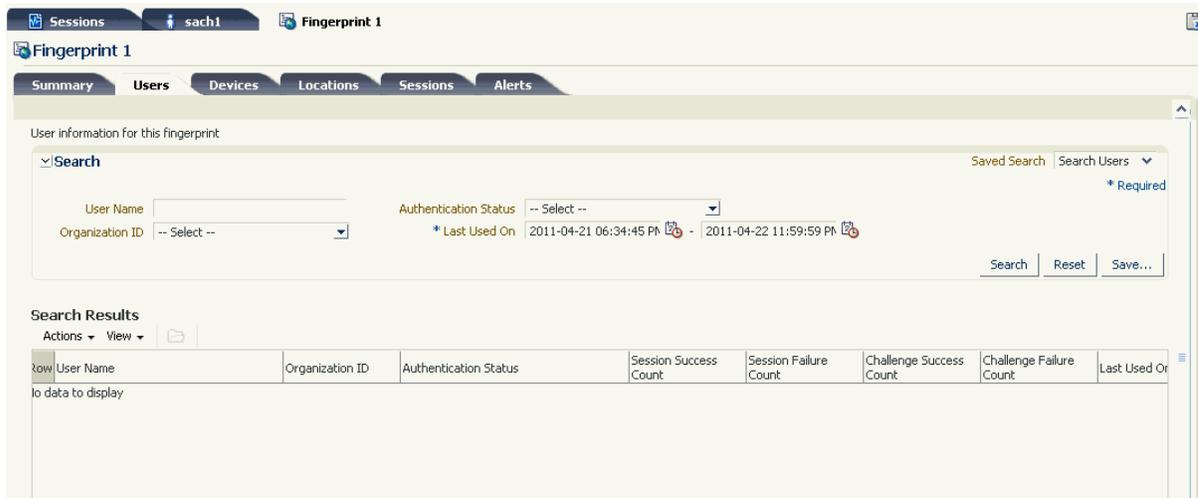


The tab contains the following filter parameters:

*Table 6–49    Fingerprint Details: Users tab*

| Filter | Description |
|---|---|
| User Name | Login name given by user to login. (Not for Fingerprint) |
| Organization ID | Identifies the organization to which the user belongs. (Not for fingerprint) |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the users who used the device to login during the given time duration. (not for fingerprint) |

## 6.14.3  Fingerprint Details: Devices Tab

This tab lists all devices for which the fingerprint was used.

*Figure 6–30   Fingerprint Details: Devices*
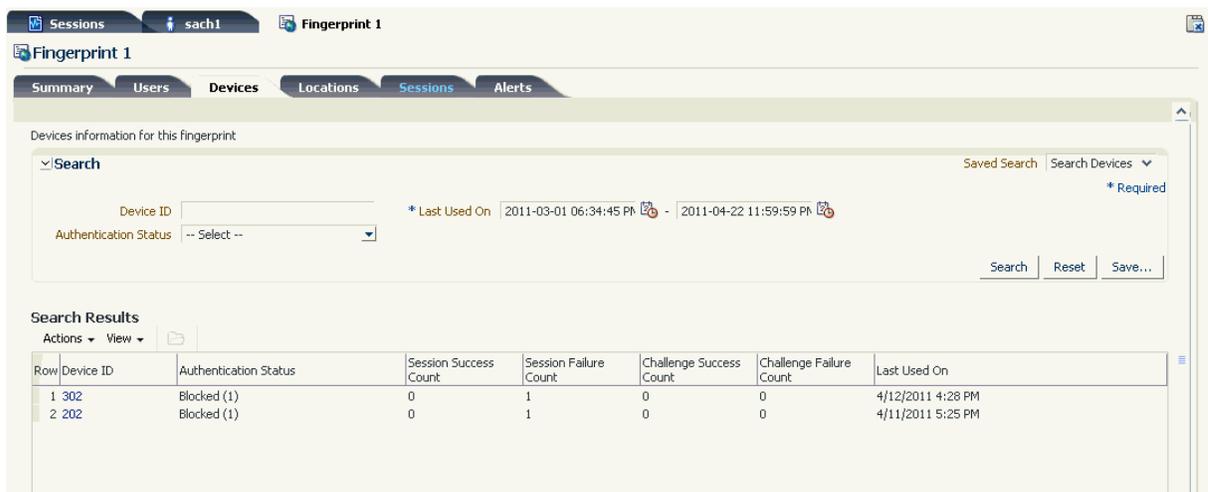


The Device tab of the Fingerprint Details page enables you to determine which devices and how many times the fingerprint was used for each device during login process.

The tab contains the following filter parameters.

**Table 6–50    Fingerprint Details: Devices Tab**

| Field | Description |
|---|---|
| Device ID | Uniquely identifies each device and is autogenerated by the application. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the devices which were used by the user to login during the given time duration. |

## 6.14.4  Fingerprint Details: Locations Tab

This tab lists all locations for which the fingerprint was used.

**Figure 6–31    Fingerprint Details: Locations**



The Locations tab of the Fingerprint Details page enables you to determine which locations and how many times the fingerprint was used for each location during the login process.

The tab contains the following filter parameters.

**Table 6–51    Fingerprint Details: Locations Tab**

| Filters | Description |
|---|---|
| Country | Country ID |
| State | State ID |
| City | City ID |

*Table 6–51  (Cont.)  Fingerprint Details: Locations Tab*

| Filters | Description |
| --- | --- |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the locations from which the user logged in during the given time duration |

## 6.14.5 Fingerprint Details: Sessions Tab

This tab lists of login sessions in which the fingerprint was generated for a particular period.

*Figure 6–32  Fingerprint Details: Sessions*



The tab contains the following filter parameters.

*Table 6–52  Fingerprint Details: Sessions tab*

| Filter | Description |
| --- | --- |
| Session ID | ID of the session. |
| Alert Message | Display name describing the alert |
| Alert Level | Severity of the alert whether high, medium, low. |
| Device ID | Unique identifier of each device autogenerated by the application. |
| User Name | Login name given by user to login. |
| Organization ID | Identifier for the organization to which the user belongs. |
| Country | Country ID |
| City | City ID |

**Table 6–52   (Cont.)  Fingerprint Details: Sessions tab**

| Filter | Description |
| --- | --- |
| State | State ID. |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Login Time | Login time of the session. Field used to get all the sessions during which the device logged in for the given time duration. |

## 6.14.6  Fingerprint Details: Alerts Tab

This tab lists alerts that have been triggered for this device within the time frame specified in the search criteria.

**Figure 6–33   Fingerprint Details: Alerts**
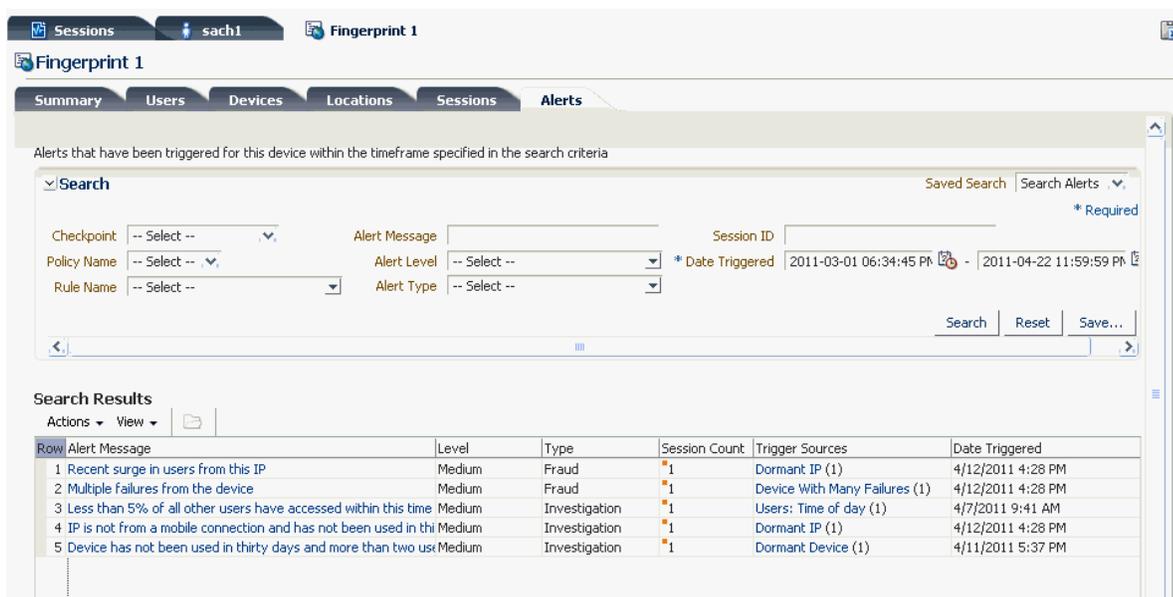


The tab contains the following filter parameters.

**Table 6–53   Fingerprint Details: Alerts Tab**

| Filter | Description |
| --- | --- |
| Checkpoint | Decision and enforcement point when the policies were called to run their rules |
| Policy Name | Name of the policy. The policy list is dynamically populated in respect to what has been selected for the checkpoint. |
| Rule Name | Name of the rule that generated the alert. |
| Alert Message | Display name describing the alert |
| Alert Level | Severity of the alert whether high, medium, low. Multiple alert levels can be selected. |

*Table 6–53 (Cont.) Fingerprint Details: Alerts Tab*

| Filter | Description |
| --- | --- |
| Alert Type | Type of the alert whether fraud, investigation, information, or other types. Multiple alert types can be selected. |
| Session ID | Unique identifier for a session |
| Date Triggered | Date the alert was triggered for this device. Required field. |

## 6.14.7 Fingerprint Details Tasks

This section describes how to obtain information through the use of the Fingerprint Details pages.

### 6.14.7.1 View flash fingerprint details

The flash fingerprint is only be available if the "flash" is installed on the client machines. To view flash fingerprint details, click the Flash Fingerprint ID link from the session details or listing page.

The Fingerprint Details page opens with additional details.

### 6.14.7.2 View browser fingerprint details

To view browser fingerprint details, click the Browser Fingerprint ID link from the session details or listing page.

The Fingerprint Details page opens with additional details.

### 6.14.7.3 Search and view the different users for which the fingerprint was used

To search and view the different users for which the fingerprint was used:

1. Click the Fingerprint ID link in the Session details or listing page.

   The Fingerprint Details page is opened and shows additional details.

2. Click the **Users** tab.

   This tab lists all the users who used the fingerprint during the time frame specified.

3. Search for the different users for which the fingerprint was used using the following filter parameters:

*Table 6–54 Fingerprint Details: Users tab*

| Filter | Description |
| --- | --- |
| User Name | Login name given by user to login. (Not for Fingerprint) |
| Organization ID | Identifies the organization to which the user belongs. (Not for fingerprint) |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the users who used the device to login during the given time duration. (not for fingerprint) |

### 6.14.7.4 Search and view the different devices for which the fingerprint was used

To search and view the different devices for which the fingerprint was used:

1. Click the Fingerprint ID link in the Session details or listing page.

The Fingerprint Details page is opened and shows additional details.

**2.** Click the **Devices** tab.

This tab lists all devices for which the fingerprint was used.

**3.** Search for the different devices for which the fingerprint was used using the following filter parameters:

*Table 6–55    Fingerprint Details: Users tab*

| Filter | Description |
| --- | --- |
| User Name | Login name given by user to login. (Not for Fingerprint) |
| Organization ID | Identifies the organization to which the user belongs. (Not for fingerprint) |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the users who used the device to login during the given time duration. (not for fingerprint) |

This report helps to find out which devices were used and how many times the fingerprint was used for each device during login process.

### 6.14.7.5 Search and view the different locations for which the fingerprint was used

To search and view the different locations for which the fingerprint was used:

**1.** Click the Fingerprint ID link in the Session details or listing page.

The Fingerprint Details page is opened and shows additional details.

**2.** Click the **Locations** tab.

This tab lists all locations for which the fingerprint was used.

**3.** Search for the different locations for which the fingerprint was used using the following filter parameters:

*Table 6–56    Fingerprint Details: Locations Tab*

| Filters | Description |
| --- | --- |
| Location | Country ID, State ID, City ID |
| IP Address | Address mapped to location |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the locations from which the user logged in during the given time duration |

This report helps to find out which locations and how many times the fingerprint was used for each location during login process.

### 6.14.7.6 Search and view all the login sessions or search login sessions for a particular period for the fingerprint

To search and view all the login sessions or search login sessions for a particular period for the fingerprint:

**1.** Click the Fingerprint ID link in the Session details or listing page.

The Fingerprint Details page is opened and shows additional details.

**2.** Click the **Sessions** tab.

This tab lists of login sessions in which the fingerprint was generated for a particular period.

**3.** Search and view all the login sessions or search login sessions by the Session Date for the fingerprint.

Searching by Session Date gets all the sessions during which the device logged in for the given time duration.

### 6.14.7.7 Navigate to other details pages for users, devices, sessions and locations

You can access other details pages from a details page:

- From the Users tab: click the User Name link to open the User Details page.

- From the Locations tab, click the Location or IP link to open the Location Details page.

- From the Devices tab: click the Device ID link to open the Device Details page.

- Links for User Name, IP address, session, and location are available on the Sessions tab.

## 6.15 Alert Details Page

The Alert Details page provides information on the message, level, type of the message and cross references on other data types such as user, device, location, sessions, browser, operating system, locales, and others. Additionally, information is provided about the generation of the alert.

The Alert Details page allows you to quickly see the relationship between not just the users who have generated the alert but also other data relationships that would be useful like locales that have been used while generating the alert.

You can open the **Alert Details** page from Alert Message links in the Sessions search page, Session Details and other details pages, and Agent cases.

*Figure 6–34   Alerts Panel*

The Alert Details page presents general information and relationships details in the following tabs:

*Table 6–57    Alert Details Tabs*

| Alert Details Tabs | Description |
| --- | --- |
| Summary | This is the general alert information |
| Users | List all users for which the alert was generated. |
| | This report helps to find out which users and how many times the alert was generated for each user during login process. |
| Devices | List all devices for which the alert was generated. |
| | This report helps to find out which devices and how many times the alert was generated for each device during login process. |
| Locations | List all locations for which the alert was generated. |
| | This report helps to find out which locations and how many times the alert was generated for each location during login process. |
| Sessions | List of login sessions in which the alert was generated for a particular period. |
| Fingerprint Data | List of fingerprints created in the login process during which the alert was generated. |

## 6.15.1 Alert Details: Summary Tab

This tab provides general information about the alert and the alert template with the current details (level/type).

*Figure 6–35    Alert Details: Summary*
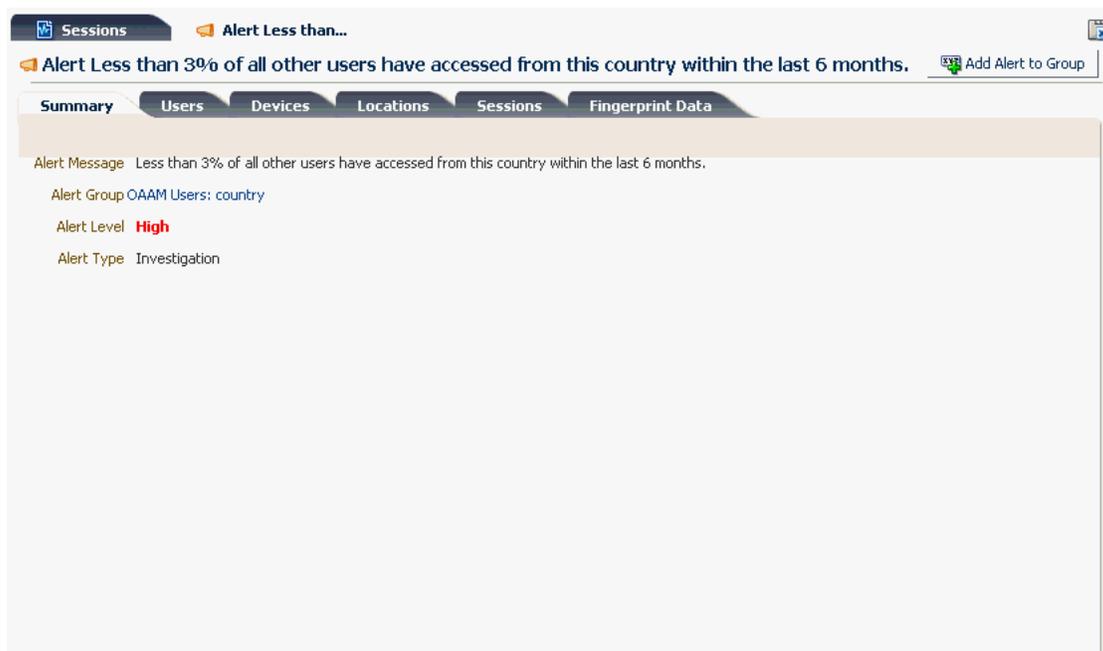


*Table 6–58    Alert Details: Summary Tab*

| Alerts Summary | Description |
| --- | --- |
| Alert Message | Text message configured in the alert. |
| Alert Type | Type of alert template currently, whether it is for fraud, investigation, information, and so on. |
| Alert Level | Severity of the alert template currently, whether it is high, medium, low. |
| Alert Group | Group with which the alert template is linked/associated. |

## 6.15.2  Alert Details: Users Tab

This tab lists the users that have a session in which the alert was triggered.

**Figure 6–36   Alert Details: Users**



The tab contains the following filter parameters.

**Table 6–59     Alert Details: Users tab**

| Filter | Description |
| --- | --- |
| User Name | Login name given by user to login. |
| Organization ID | Identifies the organization to which the user belongs. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Trigger Date | Date the alert was triggered. |

The search results display the User Name, Alert Count, and Last Date Trigger for each user. Each user is listed only one time. The Alert Count displays the number of times, the alert was triggered for the user during a time frame. By default, the results are sorted by User Name.

You can open the User Details page by clicking the User Name link.

## 6.15.3  Alert Details: Devices Tab

This tab lists the devices that have been in a session in which the alert was triggered.

*Figure 6–37   Alert Details: Devices*



The page contains the following filter parameters.

*Table 6–60   Alert Details: Device Tab*

| Field | Description |
| --- | --- |
| Device ID | Uniquely identifies each device and is autogenerated by the application. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the devices which were used by the user to login during the given time duration. |

The search results display the Device ID, Alert Count, and Last Date Trigger for each device. By default, the results are sorted by Device ID in ascending order. Each Device ID is listed only one time. Alert Count displays the number of times, the alert was triggered for the device during a time frame.

You can open the Device Details page by clicking the Device ID link.

### 6.15.4  Alert Details: Locations Tab

This tab lists the locations (country, state and city) that have been in a session in which the alert was triggered.

*Figure 6–38   Alert Details: Locations*



The page contains the following filter parameters.

*Table 6–61    Location Tab*

| Filters | Description |
| --- | --- |
| Location | Country ID, State ID, City ID |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the locations from which the user logged in during the given time duration |

The search results display the location, IP address, authentication status, last trigger date, user name, and alert count for each location. If the alert is generated from the same city but different IP then that city appears as many times as the unique IP. Alert Count displays the number of times, the alert was triggered from the location during a time frame.

You can open the Location Details page by clicking the Location link.

Clicking the User Name or IP address link opens the corresponding details page.

## 6.15.5  Alert Details: Sessions Tab

This tab lists sessions in which the alert was triggered.

*Figure 6–39 Alert Details: Sessions*



The tab contains the following filter parameters.

*Table 6–62 Sessions tab*

| Filter | Description |
| --- | --- |
| Session ID | The unique identifier for a session. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Client Type | Virtual Authentication Devices. Device or application used for authentication or fingerprinting. For example: TextPad, KeyPad, Question Pad, login page, flash tracker. auth.client.type.enum is the enum used |
| Device ID | Uniquely identifies each device and is autogenerated by the application. |
| User Name | Login name given by user to login. |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Location | Where the login occurred |
| Trigger Date | Generation date |

By default the results are sorted by Session ID, which is unique.

You can view the Session Details page by clicking the Session ID link.

Clicking the Device ID, IP address, user name, or location link opens the corresponding details page.

## 6.15.6 Alerts Details: Fingerprint Data

This tab displays the fingerprint information used when the alert was triggered during the time frame specified.

*Figure 6–40   Alert Details: Fingerprint Data*



The tab contains the following filter parameters.

*Table 6–63     User Details: Fingerprint Data Tab*

| Filters | Description |
| --- | --- |
| Fingerprint ID | Unique ID generated for fingerprint by the application |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Browser Type | The type of browser a user is viewing pages with |
| OS Type | Type of operating system |
| Locale | A set of parameters that defines the user's language, country and any special variant preferences that the user wants to see in their user interface |
| Last Date Used | Get all the fingerprints created for the given time duration |

## 6.15.7 Alert Details Tasks

This section describes how to obtain information through the use of the Alert Details page.

### 6.15.7.1 View general information about the alert

To view general information about the alert, click the alert message links from the session details, other detail pages, or agent pages.

### 6.15.7.2  View alert groups with which an alert is associated

To view the alert group with which an alert is associated:

1. Navigate to the Sessions search page.

2. Click the yellow box next to the Alert in the Search Results table.

3. Click the alert message link.

   The Alert group is displayed in the Summary tab.

### 6.15.7.3  Add alert from alert groups

To add an alert from alert groups:

1. Click the alert message links from the session details, other detail pages, or agent pages.

   The Alert Details page is displayed.

2. Click **Add Alert To Group** at the upper right corner.

   The Add Alert to Group dialog is displayed.

3. Search for the group you want to add the alert to by the group name.

   Only those groups that the alert is not a member of are displayed.

4. Select the group to add the alert to and click the **Add** button.

### 6.15.7.4  Create an alert group and add an alert to it

To create an alert group and add the alert to it:

1. Click the alert message links from the session details, other detail pages, or agent pages.

   The Alert Details page is displayed.

2. Click the **Add Alert to Group** button at the upper right corner.

   The **Add to Alert** dialog is displayed.

3. Click **Create New Group** button and specify the details for the new group.

4. Select the **Open this Group's details tab when done** option.

5. Click the **Add** button.

   The group's details tab is displayed with the alert added.

### 6.15.7.5  Search and view the different users for which the alert was generated

To search and view the different users for which the alert was generated:

1. Click the alert message links from the session details, other detail pages, or agent pages.

   The Alert Details page is displayed.

2. Click the **Users** tab.

   This tab lists the users that have a session in which the alert was triggered.

3. Search for the different users for which the alert was generated using the following filter parameters:

*Table 6–64    Alert Details: Users tab*

| Filter | Description |
| --- | --- |
| User Name | Login name given by user to login. |
| Organization ID | Identifies the organization to which the user belongs. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Trigger Date | Date the alert was triggered. |

### 6.15.7.6  Search and view the different devices for which the alert was generated

To search and view the different devices for which the alert was generated:

1. Click the alert message links from the session details, other detail pages, or agent pages.

   The Alert Details page is displayed.

2. Click the **Devices** tab.

   This tab lists the devices that have been in a session in which the alert was triggered.

3. Search for the different devices for which the alert was generated using the following filter parameters:

*Table 6–65    Device Tab*

| Field | Description |
| --- | --- |
| Device ID | Uniquely identifies each device and is autogenerated by the application. |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the devices which were used by the user to login during the given time duration. |

### 6.15.7.7  Search and view the different locations for which the alert was generated

To search and view the different locations for which the alert was generated:

1. Click the alert message links from the session details, other detail pages, or agent pages.

   The Alert Details page is displayed.

2. Click the **Locations** tab.

   This tab lists the locations (country, state and city) that have been in a session in which the alert was triggered.

3. Search for the different locations for which the alert was generated using the following filter parameters:

*Table 6–66    Location Tab*

| Filters | Description |
| --- | --- |
| Location | Country ID, State ID, City ID |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Last Used On | Get all the locations from which the user logged in during the given time duration |

### 6.15.7.8 Search and view all the login sessions or search login sessions for a particular period for the alert

To search and view all the login sessions or search login sessions for a particular period for the alert:

1. Click the alert message links from the session details, other detail pages, or agent pages.

   The Alert Details page is displayed.

2. Click the Sessions tab.

   This tab lists sessions in which the alert was triggered.

3. Search and view all the login sessions or search login sessions for a particular period for the alert using Trigger Date.

### 6.15.7.9 Search and view the fingerprints created

To search and view the fingerprints created:

1. Click the alert message links from the session details, other detail pages, or agent pages.

   The Alert Details page is displayed.

2. Click the **Fingerprint Data** tab.

   This tab displays the fingerprint information used when the alert was triggered during the time frame specified.

3. Search and view the fingerprints created by using the following filters:

*Table 6–67    User Details: Fingerprint Data Tab*

| Filters | Description |
| --- | --- |
| Fingerprint ID | Unique ID generated for fingerprint by the application |
| Authentication Status | Status of the session (each login/transaction attempt creates a new session). For information, refer to **Authentication Status**. |
| Browser Type | The type of browser a user is viewing pages with |
| OS Type | Type of operating system |
| Locale | A set of parameters that defines the user's language, country and any special variant preferences that the user wants to see in their user interface |
| Last Date Used | Get all the fingerprints created for the given time duration |

### 6.15.7.10  Navigate to other details pages for groups, users, devices, locations, sessions and fingerprints

You can open details pages from other details pages:

- From the Users tab: click the User Name link to open the User Details page.

- From the Groups tab: click the Group Name link to open the Group Details page.

- From the Locations tab, click the Location link to open the Location Details page.

- From the Devices tab: click the Device ID link to open the Device Details page.

- From the Fingerprint tab: click the Fingerprint ID to open the corresponding Fingerprint Details page.

- Links for User Name, IP address, session, and location are available on the Sessions tab.

## 6.16  Uses Cases

This section describes example use cases for the Session Details page.

### 6.16.1  Use Case: Search Sessions

You are a member of the security team at Acme Corp. You work with Oracle Adaptive Access Manager on a regular basis, following up on escalated customer issues and security alerts. You perform a session search every couple hours throughout the day to identify any issues needing your attention and it is time to perform the next search. Directions: Search for sessions in the last 24 hours that have triggered high severity alerts and where access was blocked or locked.

To search sessions:

1. Log in to OAAM Admin as an Investigator.

2. In the Navigation tree, double-click **Sessions**.

   The **Sessions Search** page is displayed.

3. Search through sessions in the last 24 hours with high alerts and a blocked or locked authentication status

   a. For **Authentication Status**, select **Blocked** and **Locked**.

   b. For **Login Time**, select the date and time, **24 hours ago**, and the current date and time.

   c. For **Alert Level**, select **High**.

   d. Click **Search**.

### 6.16.2  Use Case: Session Details Page

You see a session with a **Blocked** authentication status. This may be a case of stolen authentication credentials so you want to look into it. You open the details page for this session to take a closer look at exactly what went on in this session. You see that the login had triggered a block. Phillip, the user, was dynamically added to a high risk users group because of this rule. Directions: Part A: Drill in on the policy that caused the block to see what rules triggered. Part B: You also want to see if this user has any CSR cases related to this lockout. Search the CSR cases and determine if Phillip called in for a temporary allow.

To view session details:

1. In the **Sessions Search** page, view the **Search Results** table.

   You noticed that for Phillip, one of his sessions shows:

   - a "High alert" in the **Alerts** column. Clicking the information icon, you see a velocity alert.

   - a "Blocked" status in the **Authentication Status** column.

2. Click the **Session ID** in the **Search Results** table to open the **Session Details** page.

   In **Session Details** panel, the **Authentication Status** shows **Blocked**.

3. View the final outcomes of each checkpoint.

   a. Expand the checkpoints.

   b. View the post-authentication checkpoints.

   c. Expand the post-authentication policies.

   d. Click the policy of interest to show details about the policy.

   e. View the rules that are triggered.

   f. View the final outcomes of the rules.

      There are two final outcomes: the user is blocked and been added to a high risk group.

4. Because you want to see if Phillip has any CSR cases related to this lockout, search the CSR cases and determine if he called in to have his challenge questions reset.

   a. In the Navigation tree, double-click **Cases**. The **Cases Search** page is displayed.

   b. In **Case Type,** select **CSR**.

   c. Enter Phillip's user name into **User Name** field.

   d. In **Search Results** table, look for **Temporary Allow** in the **Last Action Type** column.

   e. Click the **Case ID** for the case that has **Temporary Allow** in the **Last Action Type** column.

   f. In the **Log** subtab of the **Case Details** page, view notes.

      The notes said he was traveling overseas when his wife asked him to look at their account online.

## 6.16.3 Use Case: Checking for Fraudulent Devices and Adding Them to a Group

### Before You Begin

Login with user who has an Investigator or Investigation Manager role.

### Checking for Fraudulent Devices and Adding Them to a Group

1. Search by action and alert to see recent blocked sessions.

   For example, search for sessions that have been blocked in the last two hours.

   You should see blocked sessions and the user who was blocked because of a device.

   For example, you see a user jsmith who was blocked because he was logging in using device 123 that had been blocked more than three times in the last 24 hours.

   2. View user details and check the Device tab to view the different devices the user used.

   For example, you compare the blocked device with other devices jsmith has used in the past. You open the user details for jsmith and view devices for the last six months. Only three devices are shown (123, 511 and 333).

   3. Compare the blocked device with other devices used using fingerprint details to see the OS, Browser, and Locale to get a general idea about the device.

   4. Check to see if the blocked device looks different than the successful ones.

   For example, you open the fingerprint details for the blocked device 123 and for device 333 that had been used recently by jsmith successfully and it showed a high number of successful uses. From the user interface, you can see that the blocked device 123 was a Linux machine with Opera running in Russian locale among other fingerprint data points.

   The device 333 is a Windows XP machine with IE running in English locale which seems to be the one the user has used most of the time recently.

   You open the fingerprint details for device 511 also and check the fingerprint data. You see it also is Windows XP machine with IE running in English locale but jsmith has not used it in a while. This makes you think device 123 was used by someone impersonating jsmith.

   5. Search sessions by Device ID to check if the device has a lot of blocked sessions and if there are a lot of different users.

   For example, you search for all the sessions device 123 has been involved in to see what other users may have been victims. There were ten sessions all in the last two weeks and many of them were blocked. As well each session was for a different user.

   6. Add the device to the blacklist group from the Sessions search tab.

   7. Export the blocked session to Excel to use as reference to contact the real users who need to reset their password.

   You export table results to Excel. The Excel sheet should contain all the session details.

## 6.16.4 Use Case: Exporting the Sessions from the Last One Week

You can export sessions to use as reference or further study and investigation.

To export sessions:

   1. Log in to the OAAM Admin.

   2. In the Sessions search page, specify one week using the date editor and click **Search**.

   3. Select the sessions from the Search Results table.

   4. From **Actions** menu, select **Export to Excel**.

   5. Click **Save File** or **Open** with and click **OK**.

   File shows Row, Session ID, Alerts, Organization ID, User name, Device ID, IP Address, Location, Authentication Status, Login Time, Pre-Authentication Score, Pre-Authentication Action, Post-Authentication Score, Post-Authentication Action, Client Type, User ID, and Internal Session ID.

### 6.16.5  Use Case: User Details, Fingerprint Details

Tom, a fraud investigator, opens the OAAM Administration Console and searches for sessions that contain high-level alerts in the last 24 hours. This search returns a number of sessions. He orders the results by the User Name column and notices "jsmith" had several sessions with the "device with implausible velocity alert". Because "jsmith" has completed registration, every session was challenged.

1. Tom opens the user details for jsmith by clicking the link in the Session page. He searches for IPs jsmith has used in the last six months. A large list of IPs is returned. It appears the jsmith has been logging in from a random location every login session.

2. Tom finds only two devices used by jsmith in the last six months in device page for jsmith.

3. Tom searches for all of jsmith's sessions in the last three months. He finds almost every session has the same device velocity alert. Tom then filters all the sessions to see how many KBA locks occurred. He finds only one.

4. Tom navigates to fingerprint details and finds that jsmith has logged in from the same browser and the same OS every time and has used the same locale also. Tom determines jsmith must be a normal user whose IP is being changed in some way. He adds jsmith to the group of "traveling users" and excludes this group from the rule that is triggering for him.

### 6.16.6  Use Case: Device and Location Details

Tom opens the OAAM Administration Console and searches for sessions that contain high-level alerts in the last 6 hours. This search returns 5 sessions.

1. Tom orders the results by the username and notices none of them are from the same user.

2. Tom then orders on IP and sees there are different IPs used in each session.

3. He then orders by the device column and sees there is one device with 2 sessions and the other devices have one session each.

4. Tom opens the device details for the device with 2 sessions. He views sessions from that device in the last month. He sees there were five sessions from this device in the last 24 hours each for a different user. The most recent session was blocked.

5. Tom opens the blocked session details to see why it was blocked. He can see that the device with maximum users in a short time frame rule triggered.

6. Tom drills in on the policy containing this rule and sees the policy and rules. The rule blocks when a device has had more than four users and from more than three cities in a 12-hour period. He goes back to the device details screen and sees that the locale is Finnish, which seems strange.

7. Tom opens another session screen and searches for sessions in the last three months using the Finnish locale. There are 23 sessions, all in the last week.

8. Ordering by location, it seems the sessions were all from unique places within Washington State. Ordering by devices however he can see there were ten devices used. Finally, ordering by username Tom could see every session was for a different user. Feeling that this was not ordinary activity Tom puts together a call list of the affected users to verify if any of the activity was valid or not.

**9.** After calling 5 users Tom sees that none of them were in the locations these sessions seemed to come from. He decides to add the Finnish locale to a watch group that causes users in that locale to be challenged with an OTP via SMS every login. He also calls the rest of the users to confirm these sessions did not belong to them.

**10.** Once sure, he also selects all the devices used and adds them to a black list group.

### 6.16.7 Use Case: IP Details and Adding to Group

George is a Big Bank user. An impersonator of George gets blocked because he was logging in from a blocked IP.

**1.** The investigator, Tom, wants to compare the IP with other IPs George has used in the past. He opens the fingerprint details for the blocked IP and for another IP George has used many times successfully.

**2.** From the user interface Tom can see that the blocked IP was a Firefox browser running in Chinese locale. The IP George seems to use most of the time is a Windows XP machine with IE running at an private locale. As a result Tom adds the IP to Restricted IPs group directly from the Sessions IP screen.

### 6.16.8 Use Case: Viewing the Sessions from a Range of IPs

To view sessions coming in from a range of IPs:

**1.** Log in to the OAAM Admin Console.

**2.** Double-click **Sessions** in the Navigation tree.

**3.** Enter the IP range in the IP range fields and click **Search**.

Sessions in the IP range are displayed in the Search Results table.

### 6.16.9 Use Case: Checking If a User Failed to Login From a Particular Device or IP

To search and view the different devices that logged in from the location get additional information like the number of times a device logged in from the location and the successful and unsuccessful login attempts from the location by each device:

**1.** From the results of a session search, click the country, state, city, or IP link.

The Location Details page for that country, state, city, or IP is displayed.

**2.** Click the **Devices** tab.

- To see additional information such as the number of times a device was used to log in from the location, search by Device ID. The Login Successes column displays the number of times a device was used to log in.

- To see the number of successful and unsuccessful login attempts from the location by each device, select Blocked and Success as the Authentication Status.

  Login failures and successes are displayed for each device.

### 6.16.10 Use Case: Checking If Users Logging In from This IP Used Spanish Browsers

To search and view the fingerprints created for the location:

**1.** From the results of a session search, click the country, state, city, or IP link.

The Location Details page for that country, state, city, or IP is displayed.

2. Click the **Fingerprint Data** tab.

3. In the Search Results table, check to see if Spanish is listed as the Locale for the Fingerprint.

## 6.16.11  Use Case: Adding Devices Used for Fraud from a Location To a Risky Group

An investigator is viewing a table of devices used from a location and decides two of them were used for fraud. He can select them and add them to a "high risk devices" group to be used in future risk evaluations. He should not lose the context of what he was doing in the process.

1. Open the OAAM Admin Console.

2. Search for sessions.

3. Open location details page.

4. Search for devices used from this location.

5. Select two devices and add them to a high risk group.

## 6.16.12  Use Case: Adding Suspicious Device to High Risk Device Group

George is a user who gets blocked because he was logging in using a device that had been blocked more than three times in the last 24 hours. Jeff, an investigator wants to compare the blocked device with other devices this user has used in the past. He opens the fingerprint details for the blocked device and for another device the user has used many times successfully. From the user interface Jeff can see that the blocked device was a Linux machine with Opera running in Russian locale. The device the user seems to use most of the time is a Windows XP machine with IE running in English locale. As a result Jeff adds the blocked device to a high risk devices group, and adds the IPs used by the device to a high risk IPs group directly from the search screen.

1. Open the OAAM Admin Console.

2. Search for sessions.

3. Open 2 device details pages.

4. View the full list of fingerprint data for both devices.

5. Select device and add it to a high risk group.

6. Select IP and add it to a high risk group.

## 6.16.13  Use Case: Mark Devices and IPs as High Risk

An investigator is searching for sessions with high alerts in the last hour. Out of the 30 sessions he thinks two were fraud so he wants to mark the devices and IPs used as high risk.

1. Open the OAAM Admin Console.

2. Search for sessions with high alerts in the last hour.

3. Select the two sessions and click the add to group button.

   A dialog appears asking what data types from these sessions to add.

4. Select devices and IPs.

   Message appears which asks the user to select a device group and an IPs group.

5. Select and add the high risk devices and high risk IPs.

A confirmation appears with message that the devices were added and that one IP was added and the other was already in the high risk IPs group.

## 6.16.14 Use Case: Search for Suspicious Sessions and Add Devices to High Risk Group

**Before You Begin**

Login with user who has a Fraud Investigator or Fraud Investigation Manager role.

**Search for Suspicious Sessions and Add Devices to High Risk Group**

Garry is an investigator searching sessions looking for suspicious situations not found by the currently configured rules. He filters for all sessions in the last month with block actions from Mexico because of a recent incident. He selects all other sessions and in a single operation adds all the devices to a high risk device group.

1. Open the OAAM Admin Console.

2. Search sessions.

3. Add to group from search page.

## 6.16.15 Use Case: Search Sessions by Alert Message

An investigator is searching for sessions with high alerts with a message containing "speed". The search returns 20 sessions containing high alerts with the following messages: "Excessive speed navigation" and "User air speed."

1. Open the OAAM Admin Console.

2. Search for sessions with high level alerts and messages containing "speed."

## 6.16.16 Use Case: Search Sessions by Geography

An investigator is searching for sessions with an ID number that starts with 40 from Los Angeles, CA, USA in the last two hours.

1. Open the OAAM Admin Console.

2. Search for sessions with an ID number starting with 40 from Los Angeles in the last two hours.

## 6.16.17 Use Case: Search by Comma Separated Values

Jeff wants to see what activity has occurred recently from a list of high risk IPs he pulled from a portal. To gauge the value of the IP data he decides to view the activity from those IPs in the last six weeks and determine if any of the activity was suspicious. Jeff starts by searching sessions that have used this comma separated list of IPs and viewing the sessions that come back.

1. Open the OAAM Admin Console.

2. Search for sessions by pasting a comma separated list of IPs into the search field and filtering to the last two weeks.

Only sessions from the IPs in the list are shown.

### 6.16.18 Use Case: Export Search Sessions Results to Excel

An investigator is searching for sessions in the last two hours. He selects five rows and exports them to Excel format document that contains all columns.

1. Open OAAM Admin Console.

2. Search for sessions.

3. Select five sessions.

4. Export them to Excel.

### 6.16.19 Use Case: Export Search Sessions Results - Export Page to Excel

An investigator is searching for sessions in the last 2 hours. He selects the column heading to select all rows and exports them to Excel format document that contains all columns.

1. Open the OAAM Admin Console.

2. Search for sessions.

3. Click the heading to select all sessions on that page.

4. Export the rows to Excel document.

# Part III

## Managing KBA and OTP

This part of the book provides information on managing Knowledge-Base Authentication (KBA) and OTP.

# 7

# Managing Knowledge-Based Authentication

This chapter introduces you to the concepts behind knowledge-based authentication (KBA), and provides information about managing tasks that impact challenge questions, validations and levels of logic algorithms used for answers, question categories, and levels of logic algorithms used for registration.

Sections in this chapter are:

- Introduction and Concepts
- Setting Up KBA Overview
- Setting Up the System to Use Challenge Questions
- Accessing Configurations in KBA Administration
- Managing Challenge Questions
- Setting Up Validations for Answer Registration
- Managing Categories
- Configuring the Registration Logic
- Adjusting Answer Logic
- Customizing English Abbreviations and Equivalences
- Customizing Abbreviations and Equivalences for Locales
- Use Cases
- KBA Guidelines and Recommended Requirements

## 7.1 Introduction and Concepts

This section describes knowledge based authentication (KBA) key concepts.

### 7.1.1 Knowledge Based Authentication

Oracle Adaptive Access Manager provides out-of-the-box secondary authentication in the form of knowledge based authentication (KBA). KBA is a secondary authentication method, an extension to the existing authentication method. It is presented after successful primary authentication (for example, a user entering a single factor credentials, such as a user name and password) to improve authentication strength.

KBA provides an infrastructure for

- Users to select questions and provide answers which are used to challenge them later on

KBA is used to authenticate an individual based on the user's answers substantiated by a real-time interactive question and answer process.

- Levels of logic algorithm for registration

  Registration Logic manages the registration of challenge questions and answers.

- Levels of logic algorithm for answers

  Answer Logic is made up of advanced matching algorithms (fuzzy logic) used by the system to intelligently detect the correct answers in the challenge response process. The algorithms and the level of Answer Logic are factors in evaluating answers.

- Validations

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

KBA is used during online authentication of the user, which is automated, or a CSR challenge where the CSR interacts with the user to authenticate him before providing CSR services.

## 7.1.2 Challenge Response Process

The KBA solution consists of securing an application using a challenge/response process where users are challenged with one or more questions to proceed with their requested sign-on, transaction, service, and so on.

## 7.1.3 Challenge Response Configuration

The challenge/response process is controlled by a combination of properties and rules.

- Question presented at random or round robin

  Presentation logic (random versus round robin) is configurable through properties. If the deployment supports Oracle Identity Manager integration, the presentation is round robin. The user is expected to answer all the registered questions online.

- The number of attempts a user is allowed for each question is set by a property.

- The total number of KBA challenge failures a user is allowed before he is locked out by Oracle Adaptive Access Manager is configured in a rule condition.

## 7.1.4 Registration

During registration, which could be enrollment, opening a new account, or another events such as a reset, the user is asked to select questions and provide answers. The order of questions that are presented to a user during the registration phase is random using configurable parameters.

Later on, the challenge questions selected at registration or during a reset may be used for challenge during high risk log ins, to access transactions, or sensitive information, or both, and so on. Oracle Adaptive Access Manager's Rules Engine and business rules are responsible for determining if it is appropriate to use challenge questions to authenticate the user.

### 7.1.5 Challenge Questions

The customer can configure a set of questions that are used to authenticate users. The Questions are grouped into several categories and the user can select questions from these categories. The out-of-the-box categories that questions can be grouped into are listed. The customer can configure questions from these categories.

- Childhood

- Sports

- Your Birth

- Parents, Grandparents, Siblings

- Automobile

- Education

- Children

- Your Employment

- Significant Other

- Pets

- Miscellaneous

During registration, users are presented with several question menus. For example, he may be presented with three question menus. A user must select one question from each menu and enter answers for them during registration. Only one question from each question menu can be registered. These questions become the user's "registered questions."

When rules in OAAM Admin trigger challenge questions, the application displays the challenge questions and accepts the answers in a secure way for users. The questions can be presented in the **QuestionPad**, **TextPad**, and other pads, where the challenge question is embedded into the image of the authenticator, or simple HTML. These are configured through properties.

### 7.1.6 Question Set

KBA offers a large pool of questions, which is the framework for obtaining answers from the user during registration or reset. The Question Set is a fixed set of questions that is allotted to the user. This set is allotted at random and once for the user unless it is reset. It is generated based on the settings configured in the Registration Logic. This Question Set prevents any single user from having access to all the challenge questions. This is to prevent a fraudster from harvesting questions for use in a phishing exercise. A user can receive a new Question Set if a customer service representative resets it for the user.

### 7.1.7 Registration Logic

Registration Logic manages the registration of challenge questions and answers. During KBA registration each user is presented with a Question Set, a subset of the challenge questions library. The Question Set is generally broken up into several drop-downs that have questions to select from. The drop-down with questions is called a "menu."

*Figure 7–1   Drop-Downs (Menus)*



The number of questions that appear on each menu, the number of categories per menu, and the number of questions that a user must register is configurable. Out-of-the-box, questions are grouped into categories. The challenge questions in the questions menus do not change unless the question set is changed. The user is required to select one question from each menu and enter answers for them. Only one question from each question menu can be registered.

Validations are applied to the answers provided by the user during registration. For example, if the question, "What year did you start junior high school," is assigned the Month-Day-Year (MMDDYY) validation, a user registering for this question is not allowed to provide "April 1st 1920" for the answer.

To configure the Registration Logic, you specify the settings for:

- The question set generation
  - The number of questions to be registered
  - The number of questions per menu
  - The number of categories per menu

  The Question Set is generated based on the Registration Logic.

- The validations that are applied to the answers

For information on setting Registration Logic, see Section 7.8, "Configuring the Registration Logic."

**How do the KBA Registration Logic Settings Affect a Customer's Question Set?**

Example configurations are presented in the following table.

| Example | Question/Menu | Categories/Menu | Questions/Category in a Menu |
|---------|---------------|-----------------|------------------------------|
| 1 | 7 | 4 | 2+2+2+1 |
| 2 | 10 | 4 | 3+3+2+2 |
| 3 | 10 | 1 | 10 |

Example #1, shown on line 1, results in registration menus containing 2 questions from category A and 2 questions from category B and 2 questions from category C and 1

question from category D. This continues in a round robin fashion as needed. If there are any categories with an insufficient number of questions or an insufficient number of categories duplicate questions can result.

The following is an example of a configuration to avoid:

- Number of questions user registers: 3

    The number of questions that a user must register. The new user registration should display the same number of question menus as the number of questions that a user must register.

- Number of questions per menu: 5

    The number of questions that appear on each menu. The new user registration should display the same number of questions in each menu as the number of categories for each menu. The total number of questions from all the menus (number of questions multiplied by the questions in each menu) cannot exceed the total number of questions available in the database.

- Number of categories per menu: 5

    The number of categories per menu. The new user registration should display the same number of categories for each menu as the number of questions in each menu.

The Question Set is the fixed set of questions that is allotted to the user. This set is allotted at random and once for the user. This is to avoid the user from discovering all the questions. In the example, fifteen or more categories are required, each with at least one question enabled. But if there are fewer than 15 categories and one of these categories has only one question enabled, some Question Sets have that question twice. The algorithm tries to use as many available categories as possible.

For example to generate a Question Set with:

- 3 menus

- 5 questions per menu

- 5 categories per menu

The algorithm tries to pick one question each from 15 categories if 15 categories are available. The minimum number of questions per category should be equal to the number of questions in the Question Set divided by the total number of categories.

### Pre-requisite for Configuring Registration Logic for Locales

The deployment administrator must ensure that there are enough questions in the database for each of the supported locale as configured in OAAM Admin during deployment; otherwise, the application displays only the English language questions during registration.

The number of locale-specific questions must be equal to or greater than the "Questions User Will Register" multiplied by the "Questions per Menu" multiplied by the "Categories per Menu."

## 7.1.8 Answer Logic

Answer Logic checks to see if the answer provided by the user matches closely to the ones provided during registration.

Answer Logic is made up of advanced matching algorithms used by the system to intelligently detect the correct answers in the challenge response process. The algorithms and the levels of logic are factors in evaluating answers.

Errors can be caused by simple input errors such as fat fingering, extra characters, misspellings, and so on. Common misspellings and abbreviations for example can be accepted if the basic information of the answer is correct.

The following algorithms are available and can be configured for your requirements:

- Phonetics
- Missing character(s)
- Extra character(s)
- Common misspellings
- Common abbreviations
- Common acronyms
- Keyboard fat fingering
- Common nicknames
- Regional spelling differences
- Date Format

The Answer Logic algorithms can be enabled or disabled and the intensity or strength of some algorithms (the level of Answer Logic used to evaluate answers given for challenge questions) can also be configured. For example, high risk transactions such as wire transfers may require a high degree of certainty (i.e. exact match) whereas accessing personal, non-sensitive information may require a lower degree of response certainty.

Answer Logic algorithms are available for both the online challenge and CSR phone challenge processes. Online settings are applied for answers the user provided online using the application. Phone challenge settings are applied for answers provided by users over the phone and entered by the CSR. The online challenge and CSR phone challenge Answer Logic are completely independent of each other. They can be configured separately.

For example, you can set the online challenge logic strength to high and the CSR phone challenge logic strength to low. For the CSR phone challenge logic strength, you may have provided more margin for error, because CSRs are listening to the answers over the phone and entering the answers.

## 7.1.9 Validations

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

There are no automated validations to ensure that question specific validations and global validations do not conflict. Administrators must take care not to configure the same validations for local and global. For example, validation for a question should not be set to numeric only if the alpha only is set as a global validation.

### Question Registration Validation (Local)

Each question can be assigned unique validations to control the answers a user is allowed to register. For example, if the business team wants to force users to answer a particular question using a specific date format.

The scope of validations applied to an individual question is local. Local validations are specified during the creation of a question.

### Global Registration Validation (Global)

Global validations control the answers a user is allowed to register for all questions. Global validations influence all answer registration. For example, if the "Four-digit year (YYYY)" validation is applied globally then only numeral answers are accepted during KBA registration. This would be a problem if there are questions available to users that would normally have alphanumeric answers.

Global validations are specified during the configuration of Registration Logic.

### Global-Local Validation

The scope of validations can be applied to individual questions or a combination of questions.

## 7.1.10  Failure Counters

Failure counters are used to lock out fraudsters so that they are unable to obtain the answers/questions.

KBA uses two failure counters. They are:

- the Online Counter
- the Phone Counter

The maximum number for online challenges and phone challenges are configurable. The phone counter maximum is "per question."

For the following example, assume:

- Max online = 3
- Max phone (per question) = 3

If the user is answering challenge questions online, and if the user is given three attempts to provide a correct answer, a total of three attempts is allowed. Each failure increments the Online Counter. The user is locked out of the session after three attempts. The online only challenge is designed to limit the exposure of questions to fraudsters.

If the user is answering challenge questions over the phone, and if the user is given three attempts at answering each question, a total of nine attempts is allowed. Each failure increments the Phone Counter. The user is locked out of the session after nine attempts.

For the next challenge, the next question is displayed. A success for an online or a phone challenge automatically resets all counters to zero.

## 7.1.11  KBA Resets

Authenticator uses questions as additional credentials to help prevent fraud. A customer service representative (CSR) can reset these questions for the user when necessary. The CSR can reset KBA-related items for a user, as described.

### 7.1.11.1 Reset Challenge Questions

The CSR resets a user's challenge questions. The system deletes the existing questions and answers and generates a new question set for the user to register from. Registration of challenge questions is required at the next log in to the Web site.

### 7.1.11.2 Reset Challenge Questions and the Set of Questions to Choose From

The CSR resets the user's challenge question set (challenge questions and the set of questions to register from). Registration of challenge questions is required at the next log in to the Web site.

### 7.1.11.3 Increment User to the Next Question

The CSR resets the user's next question so the system advances the user to the next challenge question in the list of registered questions. So if the user is currently being asked question A, question B or C is now asked. A different challenge question is presented at the next log in to the Web site.

### 7.1.11.4 Unlock a User

When the CSR unlocks the user that has been locked out of the system because of failed challenge questions. Unlocking the user resets the user's failure counter.

### 7.1.11.5 Ask Question (KBA Phone Challenge)

The CSR uses the user's challenge questions for phone authentication and enters user's response. If the user answers the question correctly, the question failure counter and increment question counter are reset. The system automatically takes appropriate action depending on the status such as unlocking the user. Information about phone and online failures is provided in Section 7.1.10, "Failure Counters." High level flows for the Ask Question action is presented in Chapter 4, "Managing and Supporting CSR Cases." The matrix in Section 7.1.10, "Failure Counters" contains detailed examples for individual flows.

## 7.1.12 Disable Question and Category Logic

This section describes the logic to handle disabled questions and categories.

**Disabling Logic**

The disabling logic is as follows for KBA:

- If you disable the last remaining question in a category, the category is automatically disabled as well.

- The number of active categories must be equal to or greater than the maximum number of categories in the question menu. An error message results when you try to disable a category and this requirement is not met.

**Consequences**

The following table summarizes the disable results.

*Table 7–1  Disable Results in Question and Category Logic*

| Disable Question or Category | New customers | user with question in question set | users with question registered |
|---|---|---|---|
| Question | The disabled question is not used to generate new users' question sets. | At re-registration or when a user changes his preference: Disabled question are replaced with another question from the same category. | The disabled question continues to be active.<br><br>If the user is re-registering or changing user preference, the disabled question is replaced with another question from the same category. |
| Category | The disabled category is not used to generate new users' question sets. | At re-registration or when a user changes his preference: All questions in the disabled category are replaced with questions from a new category that has not been used to generate current question set. | Questions from the disabled category continue to be active.<br><br>If the user is re-registering or changing user preference, all questions in the disabled category are replaced with questions from a new category that has not been used to generate the current question set. |

### 7.1.13 Locked Status

**Locked** is the status that OAAM Admin sets if the user fails the question challenge. The "Locked" status is only used if the KBA or OTP Anywhere is in use. A user is locked out of the session after the failure counter reaches the maximum number of failures. After the user is locked out, a Customer Service Representative must reset the status to **Unlocked** before the account can be used to enter the system.

## 7.2 Setting Up KBA Overview

This section outlines the steps to manage the library, registration and answer processing of the challenge questions.

### 7.2.1 Loading Challenge Questions

The challenge questions must be loaded into Oracle Adaptive Access Manager before the users can be asked to register. For information on loading challenge questions, see Section 2.6, "Importing the OAAM Snapshot."

### 7.2.2 Setting Up KBA

To set up KBA:

- Create Category

  If the out-of-the-box categories do not meet your needs, create categories that can hold relevant questions you plan to create.

  For information, see Section 7.7.2, "Creating a New Category."

- Create Questions

  Create questions that can be applicable to the users accessing your application.

  For information, see Section 7.5.3, "Creating a New Question" and Section 7.13.2, "Guidelines for Designing Challenge Questions."

- Apply Validations

Apply validations to the questions.

For information, see Section 7.6.2, "Adding a New Validation."

### 7.2.3  Setting Up Challenge

To set up challenge:

- Set up the Registration Logic - Validations are used to validate the answers given by a user at the time of registration.

  For information, see Section 7.8, "Configuring the Registration Logic."

- Set up the Answer Logic - The Answer Logic settings can be configured for the exactness required for challenge question answers and for answering threshold/tolerance, such as the level of fat fingering, typos, abbreviations, and so on.

  For information, see Section 7.9, "Adjusting Answer Logic."

### 7.2.4  User Flow

The following diagram illustrates the user experience with the KBA framework implemented.

**Figure 7–2  KBA User Flow**
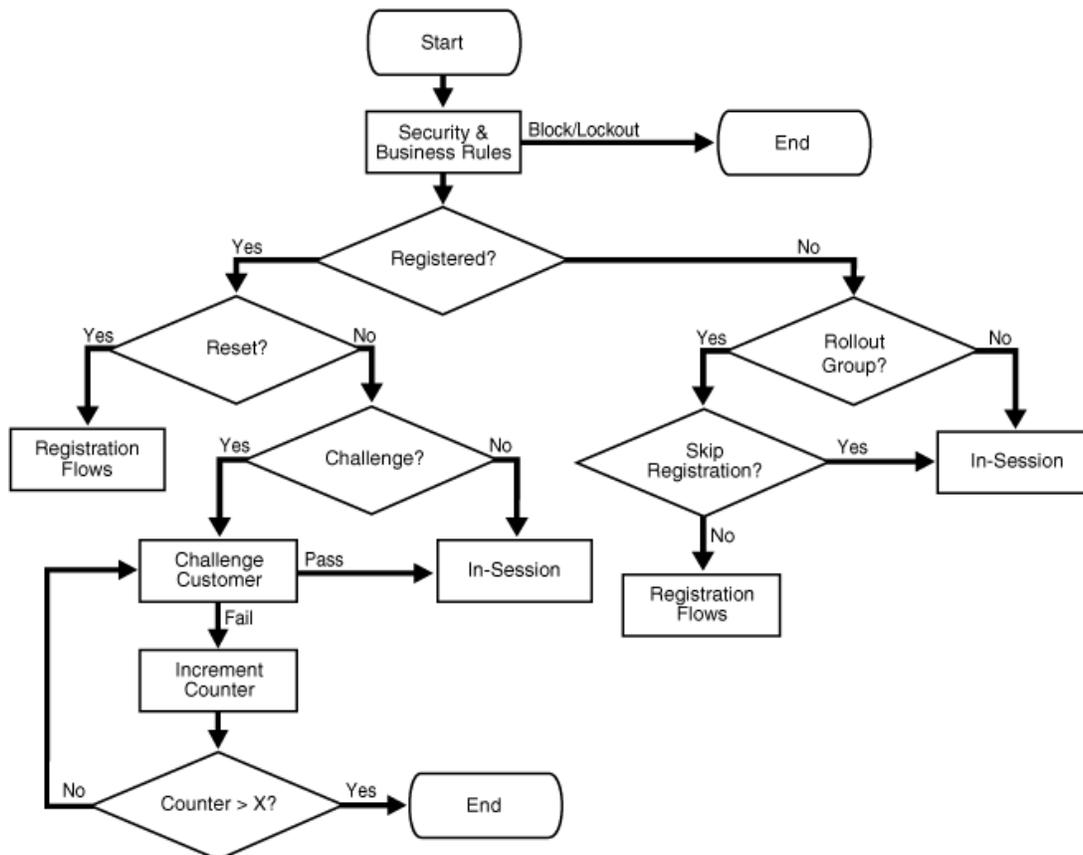
**Use Case: New User Registration**

This section illustrates an example of the new user registration experience.

The use case: You are Helen, a new Acme Corp customer. You have heard the horror stories about online identity theft and it has kept you from utilizing the online service Acme offers. This month however Acme did a customer education campaign showing the many ways customers are protected while online. You feel much better and your trust in the Acme brand has been bolstered. Today you are logging in for the first time.

Directions: Complete the registration flow to log in for the first time.

1. Open the application.

2. On the first sign in page, enter **<user name>** in the **User Name** field and press **Continue**.

3. On the second sign in page, enter **<password>** into the secure TextPad and click **Enter**.

   The **Your New Security Profile** page is displayed with information about **Security Image and Phrase** and **Security Questions and Answers**.

4. Click **Continue** to register your security profile.

   The **Your Security Device** page is displayed with a personalized virtual authentication device. On the page you are given options to learn more about your device, obtain a new image and phrase, and upgrade to a higher security device.

5. If you want, you can select a new image and phrase by clicking the **image and phrase** link or select a new device by clicking the **Upgrade** link.

   Click the **image and phrase** link until you find a device you want.

   If you clicked **Upgrade** and decided against the upgrade, you can revert to the default security device by clicking the **Revert** link.

6. Click **Continue** to accept the security device, image and phrase.

   The **Security Questions set up** page is displayed.

7. Select a question from the pull-down menu, and then answer the question in the TextPad, and click **Enter**.

8. Repeat Step 7 until you have completed selecting the questions and entering the answers.

   A welcome page appears with a message that you are successfully logged in.

**Use Case: User Login**

This section illustrates an example of the user login experience.

Use case: It has been a week since you completed the registration process on your laptop at work. Today you are on a business trip to another state and you are logging in on your laptop from using free Wi-Fi at a local coffee shop.

Directions: Try to log in to the application using a different IP (this should be a public IP and should belong to a different state).

1. Log in on your laptop using free Wi-Fi at a coffee shop in another state.

   a. On the first sign in page, enter **<user name>** in the **User Name** field and press **Continue**.

   b. On the second sign in page, enter **<password>** into the secure TextPad and click **Enter**.

A page appears asking you to answer a security question. The question appears in QuestionPad. You are asked a challenge question because the public IP group and uncommon state rules are triggered.

The public IP group rule contains the "Location: in IP group" condition and the uncommon state rule contains the "User: state first time for user" condition.

2. Enter the answer to the security question in QuestionPad and press **Enter**.

If you answer the question successfully, you are logged in.

## 7.3 Setting Up the System to Use Challenge Questions

This section provides a summary of the steps you must take to set up your system to use challenge questions.

For information on performing a phased rollout KBA and enabling challenge questions, see Chapter 8, "Enabling Challenge Questions."

| Task | [ ] |
|---|---|
| Import the OAAM Snapshot | [ ] |
| Link the appropriate policies to the user group that you want KBA to be enabled for. | [ ] |
| Ensure that KBA properties are set | [ ] |
| Enable policies for your security and business needs | [ ] |

### 7.3.1 Ensure Policies are Available

A full snapshot of policies, dependent components and configurations is shipped with Oracle Adaptive Access Manager. The snapshot is in the oaam_base_snapshot.zip file and located in the *MW_HOME/IDM_ORACLE_HOME*/oaam/init directory.

If you are using pre-packaged policies, ensure that the OAAM snapshot has been imported. If you are not using pre-packaged policies, use this chapter as a guideline for enabling challenge questions.

To import the snapshot, refer to the instructions in Section 2.6, "Importing the OAAM Snapshot."

### 7.3.2 Ensuring that KBA Properties/Default Properties are Set

Ensure that the bharosa.kba.active property is set to true. See Chapter 28, "Using the Properties Editor" for information on modifying properties.

### 7.3.3 Ensure Challenge Questions are Available

The challenge questions must be present in Oracle Adaptive Access Manager before the users can be asked to register. Challenge questions are included in the OAAM snapshot. For information on importing the snapshot which contains the questions, see Section 2.6, "Importing the OAAM Snapshot."

If you are need to use challenge questions in languages other than English, import the appropriate oaam_kba_questions_*locale*.zip files from the *MW_HOME/IDM_ORACLE_HOME*/oaam/kba_questions directory. The locale identifier *locale* specifies the language version.

### 7.3.4 Enabling Policies

Link policies that pertain to your business and security needs to a user group to which you want KBA to be enabled. For information on importing policies, see Chapter 10, "Managing Policies, Rules, and Conditions."

## 7.4 Accessing Configurations in KBA Administration

This section describes how to navigate to KBA administration tasks in OAAM Admin. You can navigate to KBA tasks through the Navigation tree. The KBA Infrastructure provides you with access to all questions, validations, categories, registration and Answer Logic, and other elements.

These are the subnodes under KBA, which provide access to the configurations in the KBA infrastructure:

- **Questions**: For managing the tasks that impact challenge questions, such as creating new questions; activating, disabling, and editing questions; and importing questions that belong to a category not currently in the system.

  Double-click **Questions** to open the **Questions Search** page.

- **Validations**: For managing the validation for the answers given by a user at the time of registration, such as creating validations based on the available validation schemes in the system, editing existing validations, and importing and exporting validations.

  Double-click **Validations** to open the **Validations Search and Edit** page.

- **Categories**: For managing the question categories in the system.

  Double-click **Categories** to open the **Categories Search** page.

- **Registration Logic**: For managing the level of logic algorithm used for the registration for challenge questions and answers.

  Double-click **Registration Logic** to open the **Registration Logic** configuration page.

- **Answer Logic**: For managing the level of logic algorithm used for answer validation.

  Double-click **Answer Logic** to open the **Answer Logic** configuration page.

For alternative methods to open search pages, refer to Section 3.9, "Search, Create, and Import." Validation Search and Edit, Registration Logic and Answer Logic pages can be opened in the same manner as the search pages.

Note that you cannot open the KBA node.

## 7.5 Managing Challenge Questions

The KBA functionality enables you to manage challenge questions.

You can perform the following task for challenge questions:

- Searching for a Challenge Question
- Viewing Question Details and Statistics
- Creating a New Question
- Creating a Question Like Another Question

- Editing a Question

- Importing Questions

- Exporting Questions

- Deleting a Question

- Disabling a Question

- Activating Questions

### 7.5.1 Searching for a Challenge Question

Use the **Questions Search** page to view a list of all challenge questions and search for a question based on various criteria. The **Questions Search** page provides access to the **Questions Details** page for any question. When the **Questions Search** page first appears, the **Search Results** table is displayed with default filter values.

To search for a question:

1.  Navigate to the **Questions Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

    An example **Questions Search** page is shown in Figure 7–3.

**Figure 7–3   Questions Search page**
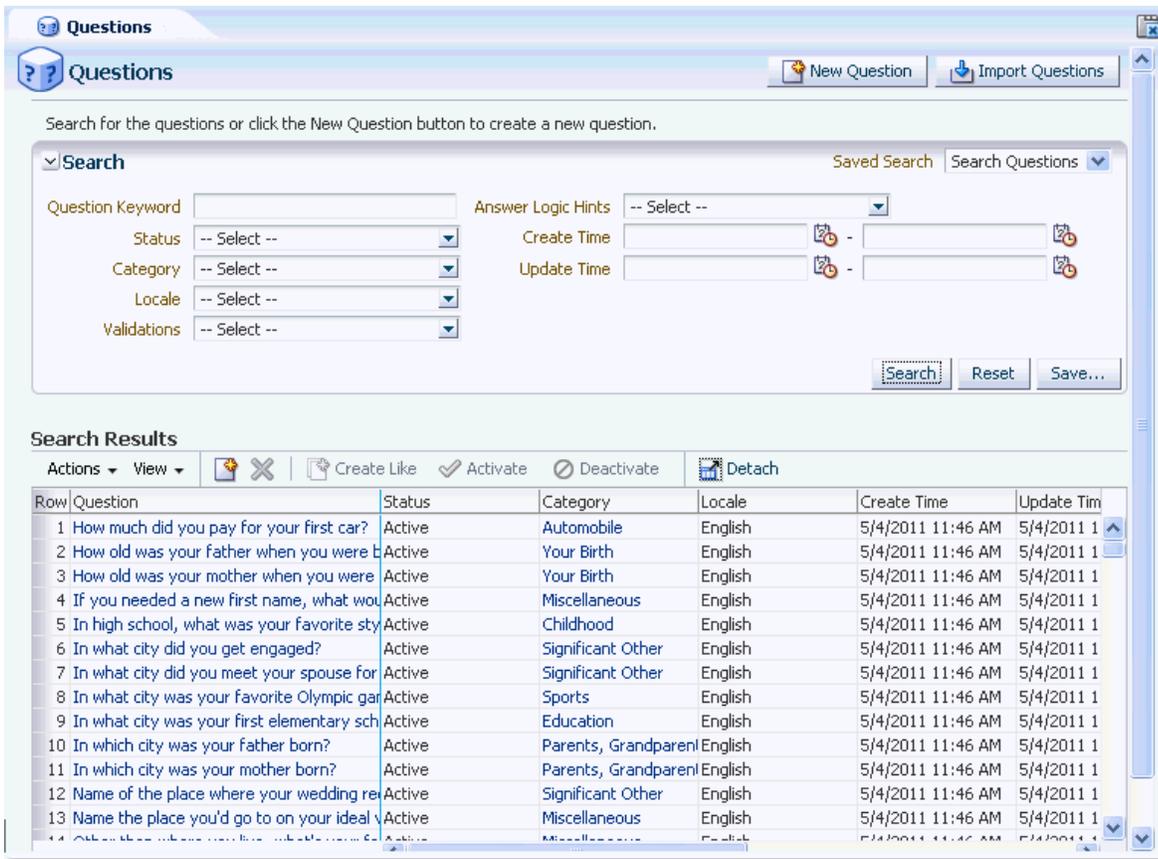


The **Questions Search** page displays a **Search** section and a **Search Results** table that shows a summary of the questions that match your search criteria.

2.  Specify criteria in the Search Filter to locate the questions and click **Search**.

The search filter criteria are described in Table 7–2.

If you want to reset the search parameters to the default setting, use the **Reset** button.

**Table 7–2    Question Search Criteria**

| Field | Description |
| --- | --- |
| Question ID | The ID for the question. |
| Question Keyword | The keyword in the question. |
| Status | The status of the question: Active or disabled. |
| Category | The category to which the question belong. For example: education, pets, sports and so on. |
| Locale | The language the question is in. For example, English, Finnish, Czech, and so on. |
| Validations | Global validations. For example: Four-digit year (YYYY), Month Day (MMDD), and so on |
| Answer Logic Hints | A hint added to questions individually to affect the Answer Logic used to evaluate given answers. For example: Date Answer Hint. |
| Created Date | A timeframe within which the question was created |
| Update Time | A timeframe within which the question was modified. |

The **Search Results** table displays a summary of questions that match the criteria specified. By default, questions are sorted on **Question Name**, but you can sort questions on **Update Time**, **Created Date**, **Status**, **Question**, and **Category**.

In the **Search Results** table, click the question link to view more details. The **Question Details** page appears.

Table 7–3, " Question Action menu commands" lists the commands that are available through the **Action** menu. You can select one or more questions and perform actions on those questions.

**Table 7–3    Question Action menu commands**

| Command | Description |
| --- | --- |
| New Question | Creates a new question. By default, the question is enabled on create. You can create a question for any locale. |
| Create Like | Creates a new case that is similar— or "like"—an existing question. |
| Edit Selected | Enables you to edit the selected question. |
| Edit Category | Opens the category of the selected question. |
| Delete Selected | Deletes questions |
| Activate Selected | Activates questions |
| Deactivate Selected | Deactivates questions |
| Import Questions | Imports questions |
| Export Selected | Exports questions as .XML files |

Except for creating a question, edit selected, and edit category, all other operations are bulk operations.

## 7.5.2 Viewing Question Details and Statistics

The **Question Details** page provides information such as:

- Question Sets with Question

- Users Registered for Question

- Percentage of Users Registered For Question

- Percentage of Successful Challenges

- Percentage of Unsuccessful Challenges

- Question ID

- Last Updated Date

To view question statistics:

1. Navigate to the **Questions Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2. From the **Questions Search** page, click the question of interest in the **Search Results** table

   The **Question Detail** page appears with the statistics.

## 7.5.3 Creating a New Question

To create a new question

1. In the Navigation tree, double-click **Questions** under **KBA**. The **Questions Search** page is displayed.

2. From the **Questions Search** page, click the **New Questions** button.

   The **New Questions** page appears where you can enter details to create a new question.

   Alternative methods to open create pages are listed in Section 3.9, "Search, Create, and Import."

   When the **New Question** page first appears, the default value for the question status is Active.

   **Question**, **Category**, **Status**, and **Locale** are required fields.

3. Pick a locale from the list of locales available.

   By default, the **Locale** menu displays English and 26 other default locale languages.

4. Type the new question in the **Question** field.

   The question names must be unique across categories.

5. From the **Category** list, select the category of question you want.

   By default, there is no data in the **Category** list. You must import the challenge questions ZIP files (oaam_kba_questions_<locale>.zip) for data to appear in the **Category** menu. You can also create a new category.

6. In the **Locale** list, select the language you want.

   By default, the **Locale** menu displays English and 26 other default locale languages.

7. Each question can be assigned unique validations to control the answers a user is allowed to register. To assign a local validation, select the validation type from the **Registration Validation** list.

   The local validations you select in this step control the answers a user is allowed to register for this particular question. It does not control the registration of answers for all questions.

   For information on the difference between global and local validations, refer to Section 7.1.9, "Validations."

8. In the **Answer Logic Hints** list, select the type of **Answer Logic Hint** you want.

   A hint can be added to questions individually to affect the Answer Logic used to evaluate given answers. This is performed to better tune the logic for the type of question. This is especially important for date related questions.

   These hints help the Answer Logic function more successfully on some questions, for example, on date related questions. If a question has the date answer hint applied then the abbreviations, phonetics and fat fingering Answer Logic runs first, and then special date format logic is applied.

9. Click **Apply**. A confirmation dialog appears telling you that the question was created successfully.

10. Click **OK** to dismiss the dialog.

    The **Question Detail** page appears for the newly created question.

    After the question has been created, you can edit details.

    > **Note:** The deployment administrator must ensure that there are enough questions in the database for each of the supported locale as configured in OAAM Admin during deployment; otherwise, OAAM Server displays only the English language questions during registration.
    >
    > The number of locale-specific questions must be equal to or greater than the "Questions User Will Register" multiplied by the "Questions per Menu" multiplied by the "Categories per Menu."

## 7.5.4 Creating a Question Like Another Question

To create a new question that is similar to an existing question:

1. Navigate to the **Questions Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2. From the **Questions Search** page, select the row corresponding to the question of interest.

3. Click the **Create Like** icon.

   The **Create Like** dialog appears with pre-populated data from the original question. Pre-populated fields are **Category**, **Locale**, **Status**, **Answer Logic Hints**, and **Registration Validations**. **Question**, **Category**, **Status** and **Locale** are required fields. The **Create Like** icon is disabled if multiple rows are selected.

   You can create a question for any locale.

4. Type the new question in the **Question** field.

**5.** Edit any of the other fields if you want.

**6.** Click **OK**.

The **Question Detail** page appears for the newly created question.

If you click **Cancel**, the **Questions Search** page appears.

### 7.5.5 Editing a Question

The **Question Details** page enables you to activate/disable questions and edit the question, question category, locale, and registration and answer validation. Read-only question statistics are available in the **Question Statistics** section. If you edit a question, users using that question receive the updated question.

To edit a question

**1.** Navigate to the **Questions Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

**2.** In the **Questions Search** page, search for the questions you are interested in.

**3.** Click the hyperlinked question you want to edit.

The **Question Details** page appears.

**4.** Make the changes you want.

You cannot edit the **Question ID** or last updated time.

**5.** Click **Apply** to save the changes or **Revert** to discard them.

If you click **Revert**, the edited details are reverted to the initial state.

### 7.5.6 Importing Questions

To import questions:

**1.** Navigate to the **Questions Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

**2.** In the **Questions Search** page, click **Import Questions** or select **Import Selected** from the **Actions** menu.

**3.** In the **Import Questions** dialog, type the path and name of the file; or use the **Browse** (...) button to locate the ZIP file that contains the questions, and then select the file.

**4.** Click **Open** and then click **Import**.

If you import questions that belong to a category not currently in the system, the category is also imported. If you import a question with the same ID number as an existing question, the existing question is overwritten.

A confirmation dialog displays the status of the operation and a list of questions that were imported into the system.

**5.** Click **Done**.

## 7.5.7 Exporting Questions

Multiple questions can be selected and exported.

To export questions:

1. Navigate to the **Questions Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2. In the **Questions Search** page, search for the questions you are interested in.

3. Select the rows corresponding to the questions of interest.

4. Select the **Export** icon or **Export** from the **Actions** menu.

5. In the **Export** dialog, click the **Export** button.

   The selected questions are exported.

## 7.5.8 Deleting a Question

To delete a question, follow these instructions.

1. Navigate to the **Questions Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2. In the **Questions Search** page, search for the questions you are interested in.

3. Select the rows corresponding to the questions of interest and click **Delete** or select **Delete Selected** from the **Actions** menu.

   The **Delete** button and **Delete Selected** menu item are enabled only if a question is selected.

   A **Confirm Delete** dialog is displayed with a list of questions and question IDs.

4. Click **Delete** to delete the questions.

   Deleted questions are not available for new registrations but users currently registered for these questions can continue to use them.

   A confirmation dialog is displayed.

5. In the confirmation dialog, click **OK**.

An error is displayed when you try to delete a question that is in used by a registered user.

When a user tries to delete multiple questions and if a few questions are associated with the user, the system bypasses the associated questions and deletes the rest and displays a message to user that the following list was not deleted. Deleted questions are not available for new registrations but the user currently registered for these questions can continue to use them.

## 7.5.9 Disabling a Question

To disable a question

1. Navigate to the **Questions Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2. In the **Questions Search** page, search for the question you want to disable.

3. Select the rows corresponding to the questions you want to disable.

4. Press the **Deactivate** button or select **Deactivate** from the **Actions** menu.

The selected questions are disabled.

Alternatively, you can disable a question by clicking the hyperlinked question on the Questions Search page, and then selecting **Disable** in the Status field on the Questions Details page.

The following scenarios occur when a question is disabled:

- The disabled question cannot be used to generate a new user's Question Set.

- At re-registration or reset, the disabled question is replaced with another question from the same category for those users who had the disabled question in their question set.

- The disable question remains active for users who have registered the question. If the user is re-registering or changing user preference, the disabled question is replaced with another question from the same category.

### 7.5.10 Activating Questions

To activate questions:

1. Navigate to the **Questions Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2. In the **Questions Search** page, search for the questions you are interested in.

3. Select the rows corresponding to the questions you want to activate.

4. Press the **Activate** button or select **Activate** from the **Actions** menu.

   The selected questions are activated.

## 7.6 Setting Up Validations for Answer Registration

You can manage and define validations that are used on answers given by users at the time of registration.

This section provides instructions to set up global validations that control the answers a user is allowed to register for all questions. For information on the difference between global and local validations, refer to Section 7.1.9, "Validations."

### 7.6.1 Using the Validations Page

The **Validations** page enables you to perform the following functions:

- Adding a New Validation

- Editing an Existing Validation

- Importing Validations

- Exporting Validations

- Deleting Validations

Navigate to the **Validations** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

An example **Validations** page is shown in Figure 7–4.

*Figure 7–4    Validations Page*



By default, validations are sorted on **Validation Name**, but you can sort validations on **Updated**.

Table 7–4, " Validation Action menu commands" lists the commands that are available through the **Action** menu. You can select one or more validations and perform actions on those questions.

*Table 7–4    Validation Action menu commands*

| Command | Description |
|---------|-------------|
| Add | Adds a new validation. |
| Import | Imports validations |
| Export | Exports validations |
| Delete | Deletes validations |

## 7.6.2  Adding a New Validation

You can add a new validation to the system when needed. Validations are defined for use during challenge questions registration.

To add a validation:

1.  Navigate to the **Validations** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2.  From the **Validations** page, click the **New Validation** button.

    The **Add a New Validation** page appears where you can enter details to create a new validation.

    Alternatively, you can open the **Add a New Validation** page by:

    ■    Selecting the **Add Validation** button from the **Search Results** toolbar.

    ■    Selecting **New Validation** from the **Actions** menu in **Search Results**.

3.  In the **Validation Type** list, select the validation scheme you want to add.

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

The parameters of the validation appears in the **Validation Parameters Details** area of the **Validations** page.

---

**Note:** ·The fields displayed on the page depends on the validation type selected.

---

4. In the **Name** field, 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.

5. Specify validation parameter that correspond to your validation type.

   For example, validation parameter can be 30 for an instance of **Maximum Length** validation. This validation instance restricts the user from entering an answer longer than 30 characters in length.

*Table 7–5   Validation Parameters*

| Validation Type | Label for Fields | Description for Validation Parameter | Example for note |
|---|---|---|---|
| Inappropriate Language | Enter Inappropriate Words | Inappropriate language for answer | Example: Sloppy, Wrong, Yucky |
| Regex | Enter Regex Pattern | Real expression pattern string for the answer. For example, pattern can be "[A-Za-z0-9]+" for Alpha-numeric validation. If the answer entered by the user is not as per the configured regular expression pattern; then, the validation fails and a configured error message is displayed. | Example: [0-9]+ |
| Date | Enter Date Notation | Date/Time pattern string for the answer. For example, the pattern can be "MMddyy" for Month Day Year validation. If the date/time answer entered by the user is not as per the configured pattern, the validation fails and a configured error message is displayed. | Example: MMDDYY |
| Minimum Length | Enter Minimum Length | Minimum length (number) for the answer. If the length of the answer entered by the user is less than the configured value, the validation fails and a configured error message is displayed. | Example: 3 |
| Maximum Length | Enter Maximum Length | Maximum allowed length (number) for the answer. If length of the answer entered by the user is above the configured value, the validation fails and a configured error message is displayed. | Example: 3 |

*Table 7–5   (Cont.)  Validation Parameters*

| Validation Type | Label for Fields | Description for Validation Parameter | Example for note |
|---|---|---|---|
| Repeated Character | Enter Number of Repeating Characters | Allowed number of repeated characters in the answer. | Example: 3 |
| | | If the answer entered by the user contains repeated characters more than the configured value, the validation fails and the user gets a configured error message. | |
| Repeated Answers | Enter Number of Repeating Answers | Allowed number of repeated answers. | Example: 1 |
| | | For example parameter value can be '1' for unique answer validation. | |
| | | If the answer entered by the user is repeated more than configured number of times, the validation fails and the user gets a configured error message. | |
| Character | Enter Disallowed Characters | Characters that are not allowed. | Example: * |

6. Click **Add**.

   OAAM Admin adds this validation instance to the list of validations in the System.

### 7.6.3  Editing an Existing Validation

To edit an existing validation

1. Navigate to the **Validations** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2. From the **Validations** page, select the hyperlinked configured validation you want to edit.

3. In the **Validation Parameter Details** section, make the necessary changes. See Table 7–5, " Validation Parameters".

   You can edit strings, numbers, and characters in the validation parameters field.

4. Click **Save**

   OAAM Admin updates this validation instance in the system.

### 7.6.4  Importing Validations

You can add a global validation to the global validation list on the Registration Logic page by importing a global validation into the system. It is added automatically to the global validation list without any notification.

### 7.6.5  Exporting Validations

To export validations:

1. Navigate to the **Validations** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2. In the **Validations** page, search for the validations you are interested in.

3. Select the rows corresponding to the validations you want to export.

4. Select **Export Selected** from the **Actions** menu.

5. When the **Export** dialog appears, select **Save File**, and then **Save**.

The file is exported and saved as a ZIP file.

### 7.6.6 Deleting Validations

To delete validations:

1. Navigate to the **Validations** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2. In the **Validations** page, search for the validations you want to delete.

3. Select the rows corresponding to the validations of interest and click **Delete**.

   A dialog appears asking you if you want to delete the validation.

4. Click **Delete** to confirm.

   A dialog appears with the message that the validation was deleted successfully.

5. Click **OK** to dismiss the dialog.

## 7.7 Managing Categories

You can perform the following task for categories:

- Searching for a Category
- Creating a New Category
- Editing a Category
- Deleting Categories
- Activating Categories
- Deactivating Categories

### 7.7.1 Searching for a Category

On the **Categories Search** page you can view a list of all categories and search for a category based on various criteria. The **Categories Search** page provides access to the **Category Details** page for any category.

When the **Categories Search** page first appears, the **Search Results** table displays results from the default search values.

To search for a category:

1. Navigate to the **Categories Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

   The **Categories Search** page displays a **Search** section and a **Search Results** table that shows a summary of the categories that match your search criteria.

2. Specify criteria in the Search Filter to locate the specific question category and click **Search**.

   The search filter criteria are described in Table 7–2.

   If you want to reset the search parameters to the default setting, use the **Reset** button.

*Table 7–6    Question Search Criteria*

| Field | Description |
|---|---|
| Category | The category name. For example: education, pets, sports and so on. |
| Status | The status of the category. |
| Created Date | A timeframe within which the category was created or modified. |
| Update Time | A timeframe within which the category was updated |

The **Search Results** table displays a summary of categories that match the criteria specified.

In the **Search Results** table, click the hyperlinked category you interested in to view more details. The **Category Details** page appears.

### 7.7.2  Creating a New Category

If the out-of-the-box categories do not meet your needs, create categories that can hold relevant questions you plan to create.

To create a new category

1.  Navigate to the **Categories Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2.  From the **Categories Search** page, click the **New Category** button or the **New** icon.

    Alternative methods to open create pages are listed in Section 3.9, "Search, Create, and Import."

    The **New Category** page appears where you can enter details to create a new category.

3.  Type the new category in the **Category** field.

4.  Enter a description.

5.  Click **Apply**.

    The **Category Details** page appears for the newly created category.

### 7.7.3  Editing a Category

The **Category Details** page enables you to changed the status, name, and description for an existing category.

To edit a category

1.  Navigate to the **Categories Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2.  In the **Categories Search** page, search for the category you are interested in.

3.  Click the hyperlinked category you want to edit.

    The **Category Details** page appears.

4.  Make the changes you want.

    Category name edits do not affect the questions already registered or new registrations.

5.  Click **Apply** to save the changes or **Revert** to discard them.

If you click **Revert**, the edited details revert to the initial state.

If questions that belonged to a category are moved to the new category, the user would be presented with the same questions.

### 7.7.4 Deleting Categories

To delete a category, follow these instructions.

1. Navigate to the **Categories Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2. In the **Categories Search** page, search for the categories you want to delete.

3. Select the rows corresponding to the categories you want and click **Delete**.

   A dialog is displayed asking if you want to delete the categories.

4. Click **Delete** to confirm.

   A dialog is displayed with a message that the categories were deleted successfully.

5. Click **OK** to dismiss the dialog.

You can delete a category if it is not referenced by questions. If the category is referenced by a question, an error message appears.

### 7.7.5 Activating Categories

To activate categories:

1. Navigate to the **Categories Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2. In the **Categories Search** page, search for the categories you want to activate.

3. Select the row for each category you want to activate.

4. Press the **Activate** button.

   A dialog is displayed with a message that the category was activated successfully.

5. Click **OK** to dismiss the dialog.

### 7.7.6 Deactivating Categories

The deactivated category is not used to generate a new question set. All questions in the deactivated category are replaced with questions from a new category that has not been used to generate a current question set at re-registration or the changing of user preferences for users with the question in their question set.

For users with the questions registered, the questions from the deactivated category continue to be active. If the user is re-registering or changing user preferences, all questions in the deactivated category are replaced with questions from a new category that has not been used to generate current question set.

To deactivate categories:

1. Navigate to the **Categories Search** page, as described in Section 7.4, "Accessing Configurations in KBA Administration."

2. In the **Categories Search** page, search for the categories you are interested in.

3. Select the row for each category you want to deactivate.

4. Press the **Deactivate** button.

A dialog is displayed with a message that the category was deactivated successfully.

5. Click **OK** to dismiss the dialog.

## 7.8 Configuring the Registration Logic

You can use Registration Logic to set up the configuration for:

- Number of questions that appear on each menu

- Number of categories per menu

- Number of questions that a user must register

- Restriction of characters entered for answers

**Configure Registration for Questions and Answers**

To configure the registration for challenge questions and answers:

1. In the Navigation tree, double-click **Registration Logic** under **KBA**. The **Registration Logic** page is displayed.

2. To enter or change the values for the question set generation, you can specify the following settings.

   - Number of questions that a customer must register

   - Number of questions that appear on each menu

   - Number of categories per menu

     The categories per menu cannot be more than the number of categories available in the system.

     **Note:**  Enter realistic numbers. For example, the number of questions that a user must register should be 3 to 7 questions

3. Click **Apply**.

   A confirmation dialog is displayed with the message, "Registration Logic details updated successfully."

4. Click **OK**.

**Add Global Validation**

To add global validations (validations you want to apply to all questions):

1. In the Navigation tree, double-click **Registration Logic** under **KBA**. The **Registration Logic** page is displayed.

2. Click the **Add** button on the results header.

   The **Add Global Validation** dialog appears.

*Figure 7–5   Add Global Validation*
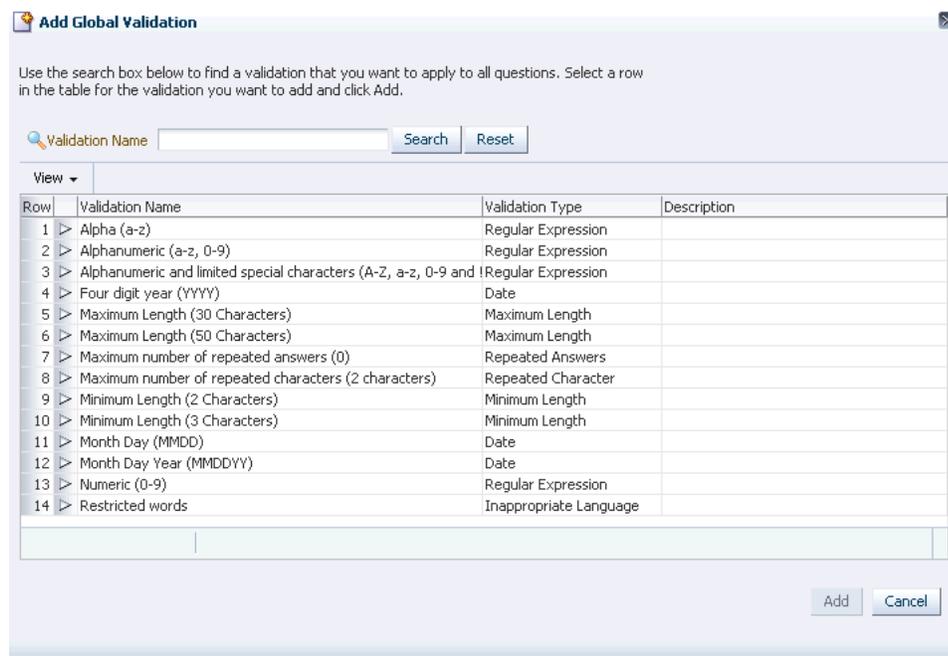


3.  In the **Add Global Validation** dialog, search for the global validations you want to add.

4.  Select the row corresponding to the validation you want to add.

    You cannot select more than one validation to add at a time.

5.  Click **Add**.

    The selected validation is added.

**Delete Global Validation**

To delete global validations (validations you do not want to apply to all questions):

1.  In the Navigation tree, double-click **Registration Logic** under **KBA**. The **Registration Logic** page is displayed.

2.  Select the rows corresponding to the validations you want to delete and then click the **Delete** button on the results header

    A dialog appears asking if you want to delete the validation.

3.  Click **Delete** to dismiss the dialog.

    A confirmation dialog appears.

4.  Click **OK** to dismiss the dialog.

# 7.9  Adjusting Answer Logic

Answer Logic, a feature of KBA, increases the usability of security questions.

## 7.9.1  About Answer Logic

Administrators can adjust how exact the challenge answers given by end users must match the answers they gave at the time of registration. If the answer given by a user

is fundamentally correct but there are minor variations such as typos, misspellings and abbreviations they should pass. The increased usability of KBA reduces or eliminates the need for unnecessary call center involvement in moderate risk situations and self service flows.

Answer Logic (fuzzy logic) algorithms can be configured 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. The algorithms are available for both the online challenge and phone challenge processes.

Out-of-the-box Answer Logic is only functional for English. Abbreviations can be globalized but creation of locale specific text equivalency files is required. For information, refer to Section 7.11, "Customizing Abbreviations and Equivalences for Locales."

### Example of How It Works

**Question**: Who was your favorite teacher in high school?

**Registered answer**: Mrs. Smith

**Given answer**: Misses Smuth

**Logic level**: If set to High, the answer is accepted.

*Table 7–7    Answer Logic Algorithm Example*

| Algorithm | Description | Reason |
|---|---|---|
| Abbreviations | This algorithm handles common abbreviations, common nicknames, common acronyms, and date format. Looks at file for allowed matches. | If the file contains Mrs=Misses, the match can be made in either direction. |
| Phonetics | This algorithm handles Answers that "sound like" the registered answer, regional spelling differences, and common misspellings | Smiith sounds like Smith |
| Keyboard fat fingering | This algorithm handles Answers with typos due to the proximity of keys on a standard keyboard. | "u" is directly to the left of "i" so it is allowed |

## 7.9.2  Common Response Errors

This section highlights the most common response errors and shows how Answer Logic algorithms are used for the system to intelligently detect the correct answers in the challenge response process. Examples of abbreviations, phonetics, and keyboard fat fingering are also provided.

### 7.9.2.1  Abbreviations

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

### Common Abbreviations

This algorithm matches the words in the following pairs as equivalent. OAAM Admin has predefined list of word-pairs that cover common abbreviations, common nicknames and common acronyms.

- Street - St.

- Drive - Dr.

- California - CA

The list can be customized by creating a new abbreviation file, `custom_auth_abbreviation_config.properties`. For information, refer to Section 7.10, "Customizing English Abbreviations and Equivalences."

**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, users 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

### 7.9.2.2 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

### 7.9.2.3 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 determines the minimum score required to match the answer with the registered answer.

> **Note:** 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

## 7.9.3 Level of Answer Logic

The level of Answer Logic, the intensity or strength of algorithms, used to evaluate answers given for challenge questions is adjustable. You can enable or disable each algorithm and you can also specify the following levels for the algorithms used:

- **Off** – No Answer Logic is used; answers must exactly match those previously registered by the user.

- **Low** – Less Answer Logic; answers provided by the user must be a match or near-match to the answers that were provided at the time of registration

- **Medium** – More Answer Logic; the user is given some leeway for the answers that are provided. For example, St. might be accepted for Street.

- **High** – Highest level of Answer Logic. The constraints are not strict for matching.

Each algorithm generates a score that represents how close the given answer is to the registered answer. OAAM Admin 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. The default thresholds are described as follows.

### 7.9.3.1 Abbreviation

For abbreviation:

- Return values: 0 or 100 (no-match OR match)

- Levels: **ON** or **OFF**

- Logic

  - If an abbreviation entry exists linking the given strings, score is 100

  - Else score is 0

### 7.9.3.2 Fat Fingering

For fat fingering:

- Return values: range 0 to 100

- Levels: **OFF**, **LOW** (90+), **MEDIUM** (75+), **HIGH** (60+)

- Logic

  - If the string lengths do not 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

### 7.9.3.3 Phonetics

For 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 DoubleMetaphone 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**

### 7.9.3.4 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
```

Assuming 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.

## 7.9.4 Configuring Answer Logic

The KBA Answer Logic tab 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.

To configure Answer Logic:

1. In the Navigation tree, double-click **Answer Logic** under **KBA**.

   You can specify different settings for Online Challenge and CSR Phone Challenge.

*Figure 7–6   Answer Logic*
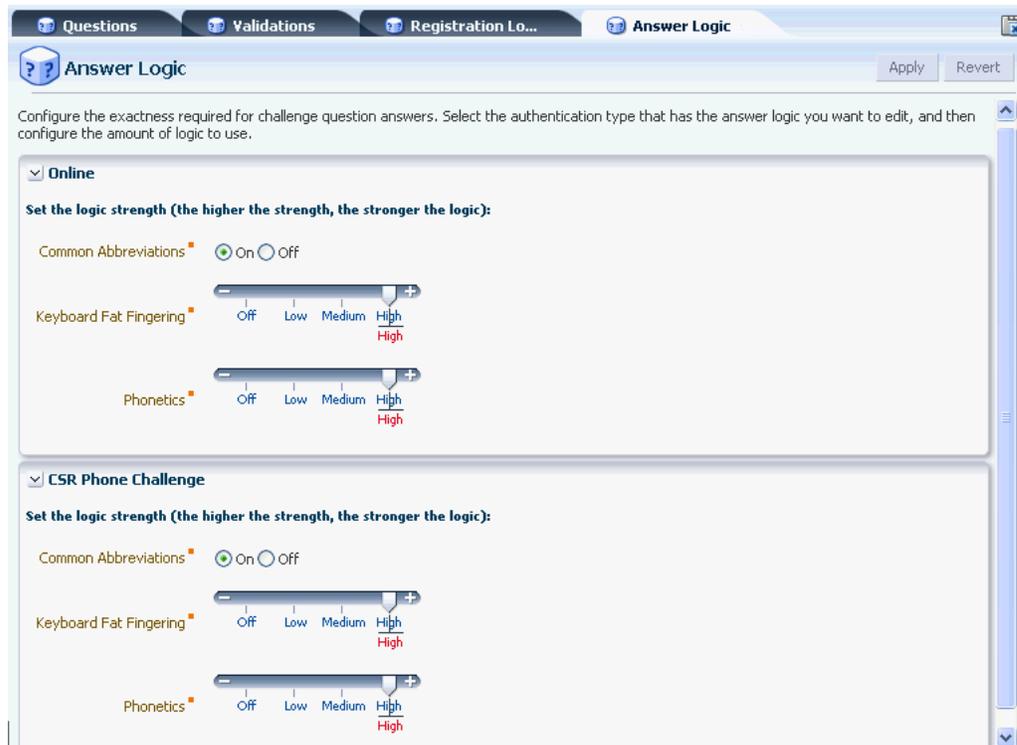


2. To change the level of Answer Logic used for keyboard fat fingering and phonetics, select **Off**, **Low**, **Medium**, or **High**: the lower the setting the higher degree of exactness required.

   For information on logic levels, see Section 7.9.3, "Level of Answer Logic."

3. Click **OK**.

## 7.10  Customizing English Abbreviations and Equivalences

Answer Logic checks if the answer provided by the user matches closely to the ones provided during registration. Answer Logic, in part, relies on pre-configured sets of word equivalents, commonly known as abbreviations.

Although there are several thousand English abbreviations and equivalences in the English version of Oracle Adaptive Access Manager, customers can perform customizations per their business requirements. For example, the customer might want the following to be considered a match.

| Registered Answer | Given Answer |
|---|---|
| nineteen hundred ninety nine | 1999 |

The out-of-the-box English abbreviations and equivalences are in a file named, `bharosa_auth_abbreviation_config.properties`. Changes cannot be made to this file.

To customize abbreviations, a new file must be created with a new set of abbreviations. This file takes precedence over the original file and all abbreviations in the original file are ignored.

To customize abbreviations:

1. Create a new abbreviation file, `custom_auth_abbreviation_config.properties`, and save it in the *IDM_ORACLE_HOME*/oaam/conf directory.

   If the `conf` folder does not exist, create one.

2. Add abbreviations and equivalences to `custom_auth_abbreviation_config.properties`.

   There are two different formats to use:

   ```
   Word=equivalent1
   Word=equivalent2
   ```

   or

   ```
   Word=equivalent1,equivalent2, equivalent3
   ```

   For example, in English, some equivalence for James are:

   ```
   Jim=James,\Jamie,\Jimmy
   ```

   With the addition of the equivalences, if a user were to enter a response as `Jim`, but had originally entered `James`, `Jim` would be accepted. Another example is that `St` may be equivalent to `Street`.

   > **Note:** Retrieval of abbreviation values is not based on the browser language; values are retrieved from the properties files.

3. Add the file to the OAAM Extensions Shared Library (`WEB-INF/classes`).

4. Using the Properties Editor, change the property, `bharosa.authenticator.AbbreviationFileName`, to point to the complete path to the file, `WEB-INF/classes/custom_auth_abbreviation_config.properties` in the extensions folder.

   The default value for the property `bharosa.authenticator.AbbreviationFileName` is `bharosa_auth_abbreviation_config.properties`. Create the `bharosa.authenticator.AbbreviationFileName` property if it does not already exist.

   Restarting the system is not necessary for the change to take effect.

   For information on using the Properties Editor, refer to Chapter 28, "Using the Properties Editor.".

5. Configure the Answer Logic by following the instructions in Section 7.9, "Adjusting Answer Logic."

If you want to revert to the original out-of-the-box abbreviations, set `bharosa.authenticator.AbbreviationFileName` back to `bharosa_auth_abbreviation_config.properties`.

## 7.11 Customizing Abbreviations and Equivalences for Locales

Locale-specific abbreviation files are shipped with OAAM. These files are named `bharosa_auth_abbreviation_config_<locale>.properties` where

`<locale>` is the locale string. For example, the Spanish version of the file is `bharosa_auth_abbreviation_config_es.properties`.

Changes cannot be made to this file. To customize abbreviations, a new file must be created with a new set of abbreviations. This file takes precedence over the original file and all abbreviations in the original file are ignored.

If you want to localize for one locale (for example, for Japanese only), perform the following steps:

1. Create one file specific to the locale with the same prefix as the original locale-specific abbreviation file. For example, `Abbreviations_ja.properties` for Japanese.

2. Add the file to the OAAM Extensions Shared Library (`WEB-INF/classes`).

3. Using OAAM, set the value of property `bharosa.authenticator.AbbreviationFileName` to that file's absolute path, `WEB-INF/classes/Abbreviations_ja.properties` in the extensions folder.

If you want customize for multiple locales, perform the following steps:

1. Create the files specific to those locales with the same prefix as the original locale-specific abbreviation file.

   For example,

   `/mydrive/IDM_ORACLE_HOME/oaam/conf/Abbreviations_ es.properties` for Spanish

   `/mydrive/IDM_ORACLE_HOME/oaam/conf/Abbreviations_ ja.properties` for Japanese

2. Add the file to the OAAM Extensions Shared Library (`WEB-INF/classes`).

3. Using OAAM, set the value of property `bharosa.authenticator.AbbreviationFileName` to that file's absolute path, `WEB-INF/classes/Abbreviations.properties` in the extensions folder.

   The locale prefix is absent in the value of the property because the locale settings of the end user's browser determine the runtime locale.

## 7.12 Use Cases

This section describes example use cases for KBA.

### 7.12.1 Use Case: Create Challenge Question

You have been asked to develop some new challenge questions to augment the existing out-of-the-box questions. Come up with a new question. Directions: Part A: Export the existing challenge questions as a backup. Part B: Create the new question in any category you like in English.

1. Log in to OAAM Admin as an administrator.

2. In the Navigation tree, double-click **Questions** under **KBA**. The **Questions Search** page is displayed.

3. In the **Questions Search** page, click the column header on the **Search Results** table to select all the rows.

**4.** Select **Export Selected** from the **Actions** menu.

**5.** In the **Export** dialog, select **Save File** and click **OK**.

**6.** Browse for the location to save the ZIP file and click **Save**.

**7.** After backing up the questions, search for the question that you are interested in.

**8.** If the question does not exist, click **New Question**. The **New Question** page is displayed.

   **Question**, **Category**, **Status**, and **Locale** are required fields.

   When the **New Question** page first appears, the default value for the question status is **Active**.

**9.** In the **Question** field, type in the question.

**10.** In the **Category** field, select a category.

**11.** Select **English** as the locale.

**12.** Select the registration validation.

**13.** Select Answer Logic hints.

**14.** Click **Apply**. A confirmation dialog appears telling you that the question was created successfully.

**15.** Click **OK** to dismiss the dialog.

   The **Question Details** page appears with information about the question and the question statistics.

**16.** After the question has been created, you can edit details.

## 7.12.2 Use Case: KBA Registration Logic

The security team has determined that it only wants to have challenge questions about sports and pets. Part A: You must log in to OAAM Admin and delete all the questions for all categories except Sports and Pets. Before doing this you should export all the challenge questions as a backup in case you want to revert. Part B: The security team has also decided that each user should register four questions and that each registration menu should contain questions from at least four categories. Configure this in OAAM Admin.

To configure KBA Registration Logic:

**1.** Log in to OAAM Admin as an administrator.

**2.** In the Navigation tree, double-click **Questions** under **KBA**. The **Questions Search** page is displayed.

**3.** Select all the questions in the **Search Results** table to export all the challenge questions as a backup in case she wants to revert.

   Clicking the # in the column header selects all rows in the **Search Results** table.

**4.** Select **Export Selected** from the **Actions** menu.

**5.** In the **Export** dialog, select **Save File** and click **OK**.

**6.** Browse for the location to save the ZIP file and click **Save**.

**7.** After the export, in the **Search Results** table of the **Questions Search** page, sort questions by **Category**.

8. Select questions that are not in the category of Sports and Pets, and click the **Delete**.

9. In the Navigation tree, double-click **Registration Logic** under **KBA**. The **Registration Logic** page is displayed.

10. In **Categories per Menu**, enter **4**.

11. In **Questions per Menu**, enter **4**.

12. In **Questions User will Register**, enter **4**.

13. Click **Apply**.

### 7.12.3 Use Case: KBA Phone Challenge

CSRs can authenticate a user by asking challenge questions over the phone. KBA Phone Challenge can be used for any registered user.

1. CSR sees the user's status (i.e. **Block**, **Locked**, and so on) and the date/time of the last login attempt when a user calls.

2. CSR requests a question with the **Ask Question** action and is presented with a challenge question and the field to enter the user's response.

3. The challenge question presented is not the same question the user has failed online if the user is currently locked out.

4. The next question in the user's registered questions is presented to the CSR.

5. The user has a limited number of over the phone attempts at each question. See Section 7.1.10, "Failure Counters" for details and examples.

6. Error messages are displayed to notify the CSR.

7. This process continues until the user runs out of questions and attempts or the user has answered a question correctly.

### 7.12.4 KBA Question Edits

Jeff is a Security Admin and needs to import and edit KBA questions in English and Spanish and add a new English question.

To do so:

1. Import KBA questions in multiple languages.

   See Section 2.6, "Importing the OAAM Snapshot."

2. Edit the questions.

   See Section 7.5.5, "Editing a Question."

3. Add a new question.

   See Section 7.5.3, "Creating a New Question."

### 7.12.5 KBA Answer Logic Edits

Jeff, a Security Admin, needs to set the KBA answer logic so sloppy users are impacted by typing errors less often.

1. Set fatfingering answer logic to high.

   See Section 7.9.3, "Level of Answer Logic."

**2.** Test against specifications.

# 7.13 KBA 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.

## 7.13.1 Best Practices for Managing Questions

### Applying Validations

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 numeral answers are accepted during KBA registration. This is a problem if there are questions available to users that normally have alphanumeric answers.

### Deleting Questions and Categories

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 users so it should be avoided.

### Questions per Menu Setting

The **Questions per menu** setting should be between 4 and 7. This range provides a good mix of questions in a question set but does not expose too many questions to any single user.

### Question User will Register Setting

The **Questions user will register** setting should be between 3 and 7. 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.

The max and min limits are configurable through the following properties.

```
bharosa.config.type.kba_config.enum.regQuestionsCount.validation.minValue=3
bharosa.config.type.kba_config.enum.regQuestionsCount.validation.maxValue=7
```

### Challenge Questions Configuration

It is recommended that you completely configure all of the challenge questions, including locale, before making the question available to users.

### Challenge Question Disabling

If you disable a challenge question, users who previously had that question continue to have the question even after it is disabled. However, users that are registering for the first time or re-registering are not presented with the disabled question.

## 7.13.2 Guidelines for Designing Challenge Questions

Guidelines for designing challenge questions are listed below:

- Question should not require answers that are personally identifiable information. For example, do not ask for Social Security Number, and other identifiers.

- Questions should not require answers that can easily be discovered via public sources such as the internet. For example, what college did you graduate from?

- Questions should not have answers that change over time. For example, what is your girlfriends name?

- Questions should not have answers that are easy to guess. For example, what is your favorite weekday?

- Questions should not be specific to any one religion, culture or sub-culture. For example, who is your favorite apostle? Which Smurf do you most closely identify with? What race would you prefer to be in the Star Wars Galaxy?

### 7.13.3 Guidelines for Answer Input

Recommended requirements for answers are listed below:

- 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.

### 7.13.4 Other Recommended Requirements

Other tips for challenge questions are:

- A unique question set should be generated for each user.

- The user should register 3-5 questions. i.e. 15 total questions to select from, 3 drop-down menus of 5 questions each.

- There should be a maximum of 2 questions from the same category.

- There should be a maximum opt-out - i.e. 3 opt-out attempts before forcing registration.

- When challenged, the same question is to be presented until the user responds correctly or question is reset by customer service agent.

# 8

# Enabling Challenge Questions

Oracle Adaptive Access Manager uses knowledge-based authentication (KBA) to prompt users for information by using challenge questions. An individual must provide previously registered answers during authentication.

This section provides guidelines for enabling challenge questions. Topics include

- What is KBA?

- Phased Approach for Registration

- Checklist for Enabling Challenge Questions

- Ensure Policies are Available

- Ensuring KBA Properties/Default Properties are Set

- Ensure Challenge Questions are Available

- Enabling Policies

- Configuring Rules for Policies

- Configuring the Challenge Question Answer Validation

- Configuring the Answer Logic

## 8.1 What is KBA?

Knowledge-based authentication (KBA) is a form of secondary authentication where during authentication, the user is prompted by challenge questions and must provide previously registered answers.

Since KBA is a secondary authentication method it should only be presented after successful primary authentication. KBA challenge is necessary in medium to high risk situations. Challenging users too often and without significant risk degrades the user experience and possibly the security. The goal is to challenge users often enough so they can successfully recall their answers but not so often that they view it as a hindrance. As well, displaying the questions excessively increases the slim possibility of exposure to fraudsters through over-the-shoulder or some other attack. In general, a challenge roughly every month for a normal user is a good rate. Suspicious users should be blocked and should not have access to the system.

## 8.2 Phased Approach for Registration

A phased rollout KBA is necessary to help ease the transition for the organization and the users. Spacing out the rollout allows for an important learning period and lessens the impact to customer service.

- The user is not registered and there is little change to the user experience.

- The user can choose to register.

- The user must register an image, a phrase, and challenge questions to be stored in a customer profile.

The most successful phased approach generally includes these phases. The first two generally last between one and three months each depending on user population size and composition.

## 8.2.1 Phase 1 - No Registration

Phase one generally consists of Oracle Adaptive Access Manager risk evaluation. In this phase there is little change to user experience. Users continue to access through the existing methods. The only slight change to user experience is a block. Blocking is recommended in the phase for extremely high-risk situations. With blocking actions applied OAAM Admin can start to prevent fraud from day one. Since only very severe security violations are blocked normal users should not experience issues with them. Phase one can last any length of time desired by the business. Generally organizations stay in phase one for one to three months.

## 8.2.2 Phase 2 - Optional Registration

Phase two is the gradual introduction of the virtual devices and secondary authentication to the user population. In this phase registration is made available to the population or sub-populations of existing users on an optional basis. This opt-in allows users to register when they have time and feel comfortable. Brand new users should be given the option to register as soon as they are created. This strategy helps to distribute load on support over a period and to add convenience for users.

### User Experience

The user is prompted to register for challenge questions after successfully authenticating at sign-on. The user can choose to bypass registration and then proceed into the session.

### Staggered Rollout

Breaking up a rollout phase into sub-groups can further ease efforts. In large deployments staggering is advised. Phase two is generally the best time to implement staggering. The most common staggering has the following steps.

- The user population is broken into groups. Geographic region is the most often used basis for this grouping

- Staggered start dates are configured for each group.

### Enable Optional Registration

To enable optional registration, link the Post-Auth Flow Phase 2 policy to the user group that you want KBA to be enabled for.

## 8.2.3 Phase 3 - Required Registration

Phase three closes the door on the opt-in registration process. This phase is the transition to normal registration procedure that is used going forward for all users. For this reason phase three has no end. Any existing users that have not registered yet must complete registration before they can access the protected applications.

**User Experience**

The user is prompted to register for challenge questions after successfully authenticating at sign-on. User proceeds into session after registration is complete.

**Enable Required Registration**

To enable required registration, link the Post-Auth Flow Phase 3 policy to the user group that you want KBA to be enabled for.

If the user group was linked to "Post-Auth Flow Phase 2" policy earlier, that linkage should be removed.

## 8.3 Checklist for Enabling Challenge Questions

The following chart presents a checklist for enabling challenge questions.

| Task | [ ] |
| --- | --- |
| Import the OAAM Snapshot | [ ] |
| Link the appropriate policies to the user group that you want KBA to be enabled for. | [ ] |
| Ensure KBA properties are set | [ ] |
| Change the rules within the registration and challenge policies with appropriate actions | [ ] |
| Configure the challenge question answer validation using OAAM Admin | [ ] |
| Configure the Answer Logic using OAAM Admin | [ ] |

## 8.4 Ensure Policies are Available

A full snapshot of policies, dependent components and configurations is shipped with Oracle Adaptive Access Manager. The snapshot is in the oaam_base_snapshot.zip file and located in the *MW_HOME*/*IDM_ORACLE_HOME*/oaam/init directory.

If you are using pre-packaged policies, ensure that the OAAM snapshot has been imported. If you are not using pre-packaged policies, use this chapter as a guideline for enabling challenge questions.

To import the snapshot, refer to the instructions in Section 2.6, "Importing the OAAM Snapshot."

## 8.5 Ensuring KBA Properties/Default Properties are Set

Ensure the bharosa.kba.active property is set to true. For instruction on how to set properties, refer to Section 28.6, "Editing the Values for Database and File Type Properties."

## 8.6 Ensure Challenge Questions are Available

The challenge questions must be present in Oracle Adaptive Access Manager before the users can be asked to register. Challenge questions are included in the OAAM snapshot. For information on importing the snapshot which contains the questions, see Section 2.6, "Importing the OAAM Snapshot."

## 8.7 Enabling Policies

Ensure that KBA security policies that pertain to your business and security needs are loaded on your system. Link them to a user group to which you want KBA to be enabled.

For example, if you want the system to be able to challenge a user over the phone through a Customer Service Representative (CSR), you must import and enable the System CC Challenge Policy.

> **Note:** If you have a policy customized, ensure that you do not import that policy again. Doing so breaks the policy that you had customized.

If you are using OAAM pre-package policies, enable phase 2 scenarios by adding the user group to which you want KBA to be enabled to Phase 2 pre- and post-authentication policies.

Phase 2 provides optional registration scenarios that you may want to try out with users. If you find that the users like to use the registration process, you may add the scenarios to your authorization process.

Phase 2 introduces much more user experience changes and includes the use of virtual authenticators for credential input. They are in charge of securely collecting the login details, and facilitating registration/challenge.

To enable Phase 2 scenarios

1.  Ensure that "Active" has been chosen for the status of the policy.

    Refer to Section 10.11, "Activate/Disable Policies."

2.  Ensure that all the rules in the policy are active.

    Refer to Section 10.23, "Activate/Disable Rule."

3.  Ensure that the user group to which you want KBA to be enabled has been selected for the Run Mode option.

    Refer to Section 10.9.1, "Linking a Policy to a Group."

    Note that it is important to ensure that the phase you are in corresponds to the policies you have your users linked to within OAAM Admin.

## 8.8 Configuring Rules for Policies

Change the rules within the registration and challenge policies with appropriate actions.

For example, assign a challenge action as one of the actions you want triggered.

For information, refer to Section 10.12.5, "Specifying Results for the Rule."

## 8.9 Configuring the Challenge Question Answer Validation

Validations are used to validate the answers given by a user at the time of registration. For answers, you can restrict the users to alphanumeric and a few specific special characters by adding a Regex validation.

For information, see Section 7.6, "Setting Up Validations for Answer Registration."

## 8.10 Configuring the Answer Logic

The Answer Logic settings can be configured for the exactness required for challenge question answers. For example, high risk transactions such as wire transfers may require a high degree of certainty (i.e. exact match) whereas accessing personal, non-sensitive information may require a lower degree of response certainty.

Configure the Answer Logic for answering threshold/tolerance, such as the level of fat fingering, typos, abbreviations, and so on.

For information, see Section 7.9, "Adjusting Answer Logic."

# 9

# Setting Up OTP Anywhere

OTP Anywhere is a secondary risk-based challenge solution consisting of a server generated one time password delivered to an end user via a configured out of band channel. Supported OTP delivery channels include short message service (SMS), email, and instant messaging.

This chapter focuses on setting up Oracle Adaptive Access Manager to use OTP for secondary, risk-based user challenges. Out of the box, OAAM provides User Messaging Service (UMS) as the delivery method. For other custom methods, refer to the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

This chapter contains the following sections:

- Introduction and Concepts
- Quick Start
- Setup Roadmap
- Prerequisites for Configuring OTP
- UMS Integration
- Enabling OTP Challenge
- Enabling Registration and Preferences
- Configuring Policies and Rules to Use OTP Challenge
- Setting Up the Registration Page
- Configuring OTP Presentation
- Configuring Failure Counter
- Customizing OTP Registration and Messaging

## 9.1 Introduction and Concepts

This section introduces you to the concept of One Time Password (OTP) and how it is used in Oracle Adaptive Access Manager.

Topics in this section are as follows:

- What is a One Time Password
- About Out-of-Band OTP Delivery
- How Does OTP Work?
- OTP Failure Counters

- [Challenge Type](#)
- [KBA vs. OTP](#)

### 9.1.1 What is a One Time Password

A one-time password is a randomly generated, single-use authentication credential. OTP is a form of secondary authentication that is used in addition to standard user name and password credentials to strengthen the existing authentication and authorization process, thereby providing additional security for users. When the user is OTP-challenged, a one-time password is generated and delivered to the user through one of the configured channels. The user must retrieve the one-time password and enter it when prompted, before the one-time password expires.

The one-time password may be either numeric or alphanumeric and any configured length and the randomization algorithm is pluggable.

The following are major benefits of using out-of-band OTP:

- The OTP is delivered to the valid user through one of the configured channels. These can include SMS, Instant Messaging (IM), and e-mail.
- The user does not require any proprietary hardware or client software of any kind.

### 9.1.2 About Out-of-Band OTP Delivery

Oracle Adaptive Access Manager 11*g* contains OTP authentication capabilities that support delivery of the OTP via the following three out-of-band channels:

- e-mail
- Short Message Service (SMS)
- instant messaging

By default, only cell phone registration is displayed on the OTP Registration page.

### 9.1.3 How Does OTP Work?

During the Registration process in OAAM, the user is asked to register for questions, image, phrase and OTP (e-mail, phone, and so on) if the deployment supports OTP. Once successfully registered, OTP can be used as a secondary authentication to challenge the user.

The administrator can enable the OTP if the deployment supports OTP. The login process begins with entering standard user name and password credentials. During a session, for example, when the user is making a large transaction, if the user is OTP-challenged, the password is delivered to the user through the configured delivery channel. The user retrieves the one-time password, then enters it.

If the correct answer is provided, the user is directed to continue with the operation. If the user answers incorrectly, he is allowed other attempts until he either answers correctly or is locked out of his account after a certain number of failures. By default, the user is allowed three attempts to provide the correct answer.

### 9.1.4 OTP Failure Counters

The failure counter is incremented when the user supplies an incorrect answer during an OTP-challenge. OTP failures are counted across sessions.

Whether the user is locked out after a number of successive OTP failures or needs to try providing the OTP again depends on the failure counter value, the maximum number for OTP challenges set by the administrator. When the failure counter exceeds this value, the user is "OTP Locked" with no further opportunity for another attempt to answer. If the user is OTP-locked, he can call the Customer Service Representative to become unlocked.

When the correct OTP is provided by the user, the failure counter is reset to 0 and the user is allowed to proceed with the operation.

### 9.1.5 Challenge Type

The challenge type is the delivery channel used to send an OTP to the user. For example, policies can challenge using OTP via the challenge type (email, SMS, or IM).

*Table 9–1    OTP Challenge Types*

| Challenge Type | Description |
| --- | --- |
| ChallengeEmail | OTP challenge via email |
| ChallengeSMS | OTP challenge via SMS |
| ChallengeIM | OTP challenge via instant messaging |

An integrator can create or configure a challenge type to handle a challenge that is required, such as generating the "secret" used for the challenge to delivering the "secret" to the user and finally validating the user's input.

The challenge type properties are used to associate a challenge type with a Challenge Processor, the java code needed to perform any work for challenges.

### 9.1.6 KBA vs. OTP

Oracle Adaptive Access Manager deployments may choose to use both KBA and OTP or each separately or no challenge mechanisms at all. If both KBA and OTP are being used in a deployment, the security team may choose to use OTP first for high risk situations and then KBA.

For example, a user logging in from a new IP addresses in a city he often logs in from is relatively low risk on its own, so a KBA challenge is a good option to gain additional verification that this is the valid user. If, however, a user is attempting a funds transfer of more than $1000 using a device and location he has never accessed from previously and the user has never performed a transfer, a stronger measure such as OTP Anywhere would be warranted.

If a customer has both KBA and OTP enabled, the priority is configurable through properties. The default is to OTP challenge first and then KBA challenge for high risk situations.

For information on KBA and OTP Anywhere priority, see Table 11–22, " OAAM Challenge Trigger Combinations".

## 9.2 Quick Start

The first step in starting to use OTP Anywhere is to enable it using the Properties Editor in OAAM Admin.

This checklist provides you with the basic steps for enabling OTP Anywhere out of the box. Included are links to pertinent documentation and prerequisites.

*Table 9–2    Quick Start for Enabling OTP Out of the Box*

| # | Task | Details |
|---|------|---------|
| 1 | Enable OTP Anywhere Registration | OTP Challenge is not enabled by default. It has to be enabled by setting the following properties to true: |
|   |   | ■ `bharosa.uio.default.register.userinfo.enabled` |
|   |   | Setting this property to true enables OTP profile in the registration flow |
|   |   | ■ `bharosa.uio.default.userpreferences.userinfo.enabled` |
|   |   | Setting this property to true enables the OTP profile in User Preferences |
| 2 | Make SMS Challenge Type Available. | Enable the SMS Challenge Type by setting the following property to true: |
|   |   | `bharosa.uio.default.challenge.type.enum.ChallengeSMS.available` |
|   |   | This makes it possible for the policies to challenge using OTP via SMS. |
| 3 | Configure UMS URLs and Credentials. | Set the following properties: |
|   |   | ■ `bharosa.uio.default.ums.integration.webservice` - UMS Web service URL |
|   |   | ■ `bharosa.uio.default.ums.integration.parlayx.endpoint` - UMS ParlayX URL |
|   |   | ■ `bharosa.uio.default.ums.integration.useParlayX=false` - Configures use of Web service or parlayx API. Value is false by default (preferred). |
|   |   | ■ `bharosa.uio.default.ums.integration.userName` - UMS integration user name |
|   |   | ■ `bharosa.uio.default.ums.integration.password` - UMS integration password |

## 9.3  Setup Roadmap

Table 9–3 lists the high-level tasks for configuring OTP for use with OAAM.

*Table 9–3    OTP Setup Tasks*

| Number | Task | Information |
|--------|------|-------------|
| 1 | Enable and configure User Messaging Service (UMS) for SMS delivery gateways on the SOA that the OAAM Server is configured to send messages through and the SMS delivery channel. <br><br> UMS comes with a number of drivers that handle traffic for a specific channel. Configure UMS to use SMS for sending the one-time password. | Section 9.4, "Prerequisites for Configuring OTP." |
| 2 | Set up UMS URLs and credentials so that OAAM can communicate with the UMS server via web services APIs to send the OTP code to the user via the challenge type. | Section 9.5, "UMS Integration." |
| 3 | Enable the SMS challenge type so that it can be used to challenge the user if secondary authentication is required. | Section 9.6, "Enabling OTP Challenge." |
| 4 | Enable registration and user preferences. The user can use the pages for profile registration and resetting OTP profile. | Section 9.7, "Enabling Registration and Preferences." |

*Table 9–3   (Cont.)  OTP Setup Tasks*

| Number | Task | Information |
|--------|------|-------------|
| 5 | Make sure out-of-the-box policies are available and active. | Section 9.8, "Configuring Policies and Rules to Use OTP Challenge." |
| 6 | Set up the registration and preferences page input fields for the user. Input properties includes maximum length for the email address the user can enter, validation for the email address field (expression), and so on.<br><br>Note: Any user facing strings need to be duplicated into resource bundle. | Section 9.9, "Setting Up the Registration Page." |
| 7 | Define type of device for the specific type of challenge. | Section 9.10, "Configuring OTP Presentation." |
| 8 | Customize the registration page using the resource bundle (client_resource_<locale>.properties file). Also, the challenge type message subject, the body of the message, and the message itself could be fully customized by specifying the custom values in resource bundle files and deploying the changes via OAAM extension shared libraries | Section 9.12, "Customizing OTP Registration and Messaging." |
| 9 | Customize OTP generation. | Section 9.13, "Customizing One-Time Password Generation." |

## 9.4  Prerequisites for Configuring OTP

Ensure that the following prerequisites are met before configuring OTP for your application:

- Install SOA Suite
- Configure the Delivery Channels

Figure 9–1 shows an OTP implementation.

*Figure 9–1   An OTP Implementation*
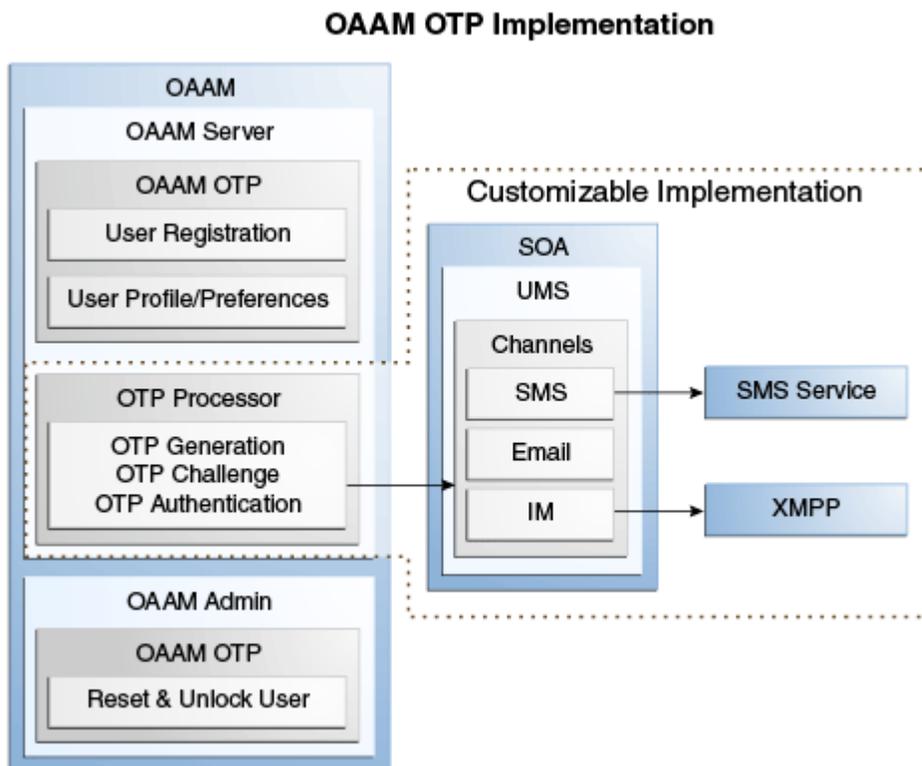


### 9.4.1  Install SOA Suite

The Oracle SOA Suite contains the User Messaging Service (UMS). Before you can configure the Oracle User Messaging Service (UMS) driver and OTP, you must have installed the SOA Suite 11*g*, configured the SOA Domain and have the Admin Server and the SOA Server running. You also need access to the Oracle Enterprise Manager Fusion Middleware Control Console.

For information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

### 9.4.2  Configure the Delivery Channels

In addition to the components that comprise the User Messaging Service (UMS) itself, the other key entities in a messaging environment are the external gateways required for each messaging channel. These gateways are not a part of the User Messaging Service (UMS) or Oracle WebLogic Server. Since UMS drivers support widely-adopted messaging protocols, UMS can be integrated with existing infrastructures such as an e-mail servers or XMPP servers. Alternatively, UMS can connect to outside providers of SMS service that support SMPP.

UMS must be configured for appropriate delivery gateways on the SOA that the OAAM Server is configured to send messages through.

*Figure 9–2   Messaging Service*
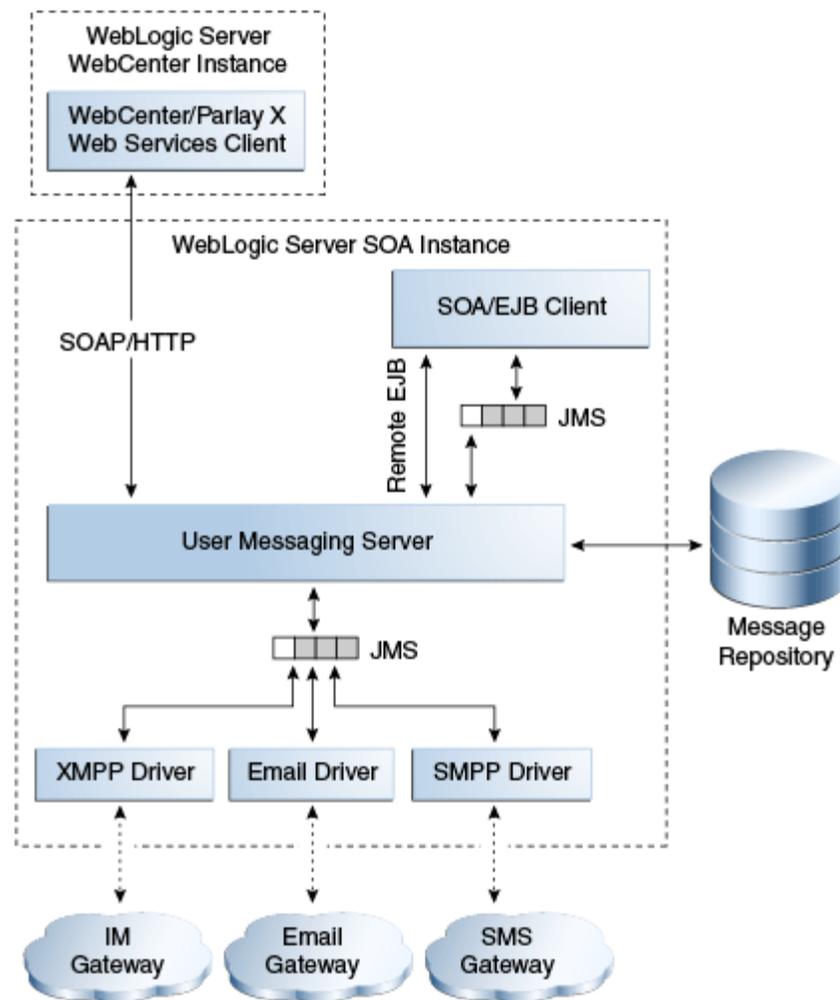


UMS Drivers connect UMS to the messaging gateways. The drivers handle traffic for a specific channel. They need to be configured with the properties of the appropriate delivery server, protocol, and so on from which messages are sent. The OAAM Server will be set up for the channels. To configure drivers, follow the steps in "Configuring User Messaging Service Drivers" in *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

### 9.4.2.1  Email Driver

Configure the Email driver to a SMTP server as described in "Configuring the Email Driver" in *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*. You will need to provide parameter values for connecting to the remote gateway.

*Table 9–4    Connecting to the SMTP Server*

| Parameter | Description |
| --- | --- |
| OutgoingMailServer | Mandatory if email sending is required. For example, `smtp.`*name*`.com` for *name*. |
| OutgoingMailServerPort | Port number of SMTP server. |
| OutgoingMailServerSecurity | Possible values are TLS and SSL. |
| OutgoingDefaultFromAddress (optional) | The email address that is indicated as the sender of the email message. |
| OutgoingUsername | The user account from which the email is sent. |
| OutgoingPassword | The account's password (stored in encrypted format). |

Press **Apply**. To have these settings take effect, the driver has to be restarted.

### 9.4.2.2  SMPP Driver

Short Message Peer-to-Peer (SMPP) is one of the most popular GSM SMS protocols. User Messaging Service includes a prebuilt implementation of the SMPP protocol as a driver that is capable of both sending and receiving short messages.

> **Note:**   For SMS, unlike the Email driver that is deployed out-of-the-box, you need to deploy the SMPP driver first before modifying the configurations.

Configure the SMPP driver as described in the "Configuring the SMPP Driver" section of the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite*. You will need to provide parameter values for connecting to the driver gateway vendor.

*Table 9–5    Connecting to the Vendor*

| Parameter | Description |
| --- | --- |
| SmsAccountId | The Account Identifier on the SMS-C. This is your vendor account ID which you need to get from the vendor. |
| SmsServerHost | The name (or IP address) of the SMS-C server. TransmitterSystemId |
| TransmitterSystemPassword | The password of the transmitter system. This includes Type of Password (choose from Indirect Password/Create New User, Indirect Password/Use Existing User, and Use Cleartext Password) and Password. This is the password corresponding to your vendor account ID |
| TransmitterSystemType | The type of transmitter system. The default is Logica. |
| ReceiverSystemId | The account ID that is used to receive messages. ReceiverSystemPassword |
| ReceiverSystemType | The type of receiver system. The default is Logica. |
| ServerTransmitterPort | The TCP port number of the transmitter server. |
| ServerReceiverPort | The TCP port number of the receiver server. |
| DefaultEncoding | The default encoding of the SMPP driver. The default is IA5. Choose from the drop-down list: IA5, UCS2, and GSM_DEFAULT. |
| DefaultSenderAddress | Default sender address |

## 9.5 UMS Integration

Set up OAAM to use the UMS server by modifying the following properties using the Properties Editor. The properties to set for the UMS server URLs and credentials are shown in Table 9–6. After you set up the UMS server properties, restart the application.

Note: End point is the Web Services URL that OAAM uses to send calls into UMS.

*Table 9–6    UMS Server URLs and Credentials*

| Property | Default Value | Description |
| --- | --- | --- |
| bharosa.uio.default.ums.integration.webservice | | UMS Server Web service URL |
| | | http://<UMS Server URL>:<UMS Port>/ucs/messaging/webservice |
| bharosa.uio.default.ums.integration.parlayx.endpoint | | UMS Server ParlayX Endpoint URL |
| | | http://<UMS Server URL>:<UMS Port>/sdpmessaging/parlayx/SendMessageService |
| bharosa.uio.default.ums.integration.useParlayX | false | Configures the use of web service or parlayx API. The value is false by default (Web services recommended) |
| bharosa.uio.default.ums.integration.userName | | User name for UMS server |
| bharosa.uio.default.ums.integration.password | | Password for UMS server |
| bharosa.uio.default.ums.integtaion.policies | | UMS authentication policies |
| bharosa.uio.default.ums.integration.fromAddress | demo@company.example.com | OAAM from address for OTP messages |
| bharosa.uio.default.ums.integration.message.status.poll.attempts | 3 | Number of times to attempt status poll each time the wait page is displayed |
| bharosa.uio.default.ums.integration.message.status.poll.delay | 1000 | Delay between status polls while the wait page is being displayed |
| bharosa.uio.default.ums.integration.sleepInterval | 10000 | |
| bharosa.uio.default.ums.integration.deliveryPage.delay | 3000 | |

After you set up the UMS server properties, restart the application.

## 9.6 Enabling OTP Challenge

The challenge type is the channel that OTP can use to challenge the user, such as Email, SMS, IM, and so on. The challenge type properties are used to associate a Challenge Type with a Challenge Processor, the java code needed to perform any work for challenges.

Enable the OTP challenge type you want to use to challenge the user if secondary authentication is required by setting the available flag. Set `bharosa.uio.default.challenge.type.enum.ChallengeSMS.available` to `true`.

Then, you can define the properties for the OTP challenge type, such as the required field for registration, and register the challenge processor that is handling the challenge processing.

To enable and define a challenge type, such as ChallengeEmail, ChallengeSMS, ChallengeQuestion, and so on, perform the following steps:

1. Log in to OAAM Admin.

2. In the Navigation tree, double-click **Properties** under the **Environment** node. The
   **Properties Search** page is displayed.

3. Search for `bharosa.uio.default.challenge.type.enum` and edit the
   properties for the out-of-the-box OTP challenge type:

**SMS Challenge Type**

The following is an example of an enum defining SMS challenge for OTP:

*Table 9–7 Properties for SMS Challenge Type*

| Property | Default Value | Description |
| --- | --- | --- |
| bharosa.uio.default.challenge.type.enum.ChallengeSMS | 2 | SMS Challenge enum value |
| bharosa.uio.default.challenge.type.enum.ChallengeSMS.name | SMS Challenge | Name of SMS challenge type |
| bharosa.uio.default.challenge.type.enum.ChallengeSMS.description | SMS Challenge | Description of SMS challenge type |
| bharosa.uio.default.challenge.type.enum.ChallengeSMS.processor | com.bharosa.uio.processor.challenge.ChallengeSMSProcessor | Processor class for SMS challenge type. Specifies the java class for handling challenges of this type. The challenge mechanism is customizable through Java classes. See the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager* for information. |
| bharosa.uio.default.challenge.type.enum.ChallengeSMS.requiredInfo | mobile | Required fields to challenge user with SMS challenge type. A comma separated list of inputs from registration input enum |
| bharosa.uio.default.challenge.type.enum.ChallengeSMS.available | false | Availability flag for SMS challenge type. Specifies if the challenge type is available for use (service ready and configured). To enable/disable an OTP challenge type, the available flag should be set. |
| bharosa.uio.default.challenge.type.enum.ChallengeSMS.otp | true | OTP flag for SMS challenge type |

**Email Challenge Type**

The following is an example of the enum defining the challenge type, email challenge, for OTP:

*Table 9–8 Properties for Email Channel Type*

| Property | Default Value | Description |
| --- | --- | --- |
| bharosa.uio.default.challenge.type.enum.ChallengeEmail | 1 | Email Challenge enum value |
| bharosa.uio.default.challenge.type.enum.ChallengeEmail.name | Email Challenge | Name of email challenge type |
| bharosa.uio.default.challenge.type.enum.ChallengeEmail.description | Email Challenge | Description of email challenge type |

*Table 9–8   (Cont.)  Properties for Email Channel Type*

| Property | Default Value | Description |
|---|---|---|
| bharosa.uio.default.challenge.type.enum.ChallengeEmail.processor | com.bharosa.uio.processor.challenge.ChallengeEmailProcessor | Processor class for email challenge type |
| | | Specifies the java class for handling challenges of this type. The challenge mechanism is customizable through Java classes. See the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager* for information. |
| bharosa.uio.default.challenge.type.enum.ChallengeEmail.requiredInfo | email | Required fields to challenge user with email challenge type |
| | | A comma separated list of inputs from registration input enum |
| bharosa.uio.default.challenge.type.enum.ChallengeEmail.available | false | Availability flag for email challenge type |
| | | Specifies if the challenge type is available for use (service ready and configured). To enable/disable an OTP challenge type, the available flag should be set. |
| bharosa.uio.default.challenge.type.enum.ChallengeEmail.otp | true | OTP flag for email challenge type |

## 9.7 Enabling Registration and Preferences

For the end user to be able to enter his profile and reset phases at a later time, the following properties must be enabled so that the fields that are set up for the pages can be used.

1. Ensure that the OTP Challenge types are enabled.

2. Use the Properties Editor in the OAAM Admin to enable OTP profile registration and preference setting. The properties are listed below.

*Table 9–9   Enable OTP Profile Registration and Preference Setting*

| Property | Description |
|---|---|
| bharosa.uio.default.register.userinfo.enabled | Setting the property to true enables the profile registration pages if the OTP channel is enabled and requires registration. |
| bharosa.uio.default.userpreferences.userinfo.enabled | Setting the property to true enables the user to set preferences if the OTP channel is enabled and allows preference setting. |
| | User Preferences is a page that allows the user to change their image/phrase, challenge questions, un-register devices, and update their OTP profile. |

## 9.8 Configuring Policies and Rules to Use OTP Challenge

Policies in the Challenge checkpoint determine the type of challenge to present the user. For more information, refer to Section 11.5.9, "OAAM Challenge."

To configure a policy with a rule that OTP-challenge users for specific scenarios, perform the following steps:

1. Log in to the OAAM Administration Console.

2. Double-click **Policies** in the Navigation pane.

   The Policies Search page displays.

3. In the **Policies Search** page, click the **New Policy** button.

   The **New Policy** page appears. In the **Summary** tab, create a post-authentication security policy:

   a. For Policy Name, enter **OTP Challenge for Many Failures**.

   b. For **Description**, enter a description for the policy.

   c. For **Checkpoint**, select **Post-Authentication**.

   d. Modify the policy status, scoring engine, and weight according to your requirements.

   e. Click **Apply**.

   f. Click **OK** to dismiss the confirmation dialog.

4. Click the Rules tab to select it.

   a. Add general summary information about the rule.

   b. On the conditions tab, add `User: Check OTP failures` condition or other OTP-related conditions.

5. On the Results tab, specify `OAAM challenge` as the Action group.

6. Link the policy to all users.

## 9.9 Setting Up the Registration Page

Setting up the registration page involves the following tasks:

- Enabling the Opt-Out Feature
- Customizing Terms and Conditions
- Configuring Text and Fields on Registration and Preference Pages
- Customizing Registration Page Messaging

### 9.9.1 Enabling the Opt-Out Feature

The Opt-Out feature is disabled by default. To enable Opt Out for the user, set the property to `true`.

*Table 9–10   OTP opt-out properties*

| Property | Default Value |
| --- | --- |
| bharosa.uio.default.otp.optOut.enabled | false |
| bharosa.uio.default.otp.optOut.managerClass | com.bharosa.uio.manager.user.DefaultContactInfoManager |

If you want the user to be able to opt-out of registering an OTP profile, you must enable a **Decline** button on the OTP registration page by setting the following properties using the Properties Editor:

*Table 9–11    Enabling Opt-Out for OTP Registration and Challenge*

| Property | Value |
| --- | --- |
| bharosa.uio.default.register.userinfo.decline.enabled | true |
| bharosa.uio.default.userpreferences.userinfo.decline.enabled | true |

> **Note:**   The property to opt-out must be set to `true` for the **Decline** button to be available. If the other two properties are true and opt-out is `false`, the button will not be displayed.

If a customer chooses to decline registration of an OTP profile, he will not be asked again to register OTP, and he will not receive OTP challenges. However if a customer representative resets a user's OTP profile through a reset all, the user will have an opportunity to register OTP again. Even if the user has opted out of OTP registration and challenge, he can still access the OTP page in User Preferences and register for OTP.

## 9.9.2 Customizing Terms and Conditions

To configure terms and conditions check boxes and fields in the OTP registration page, add the properties in the sections following.

To configure check boxes and fields, follow these steps:

1.  Create a work folder called `oaam_extensions`. (The folder can be created anywhere as long as it is outside the installation folder.)

2.  Locate `oracle.oaam.extensions.war`, which is located in the *IAM_ Home*/oaam/oaam_extensions/generic directory.

3.  Explode `oracle.oaam.extensions.war` into the `oaam_extensions` folder.

4.  Open the `oaam_custom.properties` file in the `WEB-INF/classes/bharosa_ properties` directory of the `oracle.oaam.extensions.war` file.

5.  Add properties from Section 9.9.2, "Customizing Terms and Conditions" and Section 9.9.3, "Configuring Text and Fields on Registration and Preference Pages."

6.  Repackage `oracle.oaam.extensions.war` from the parent folder of `oaam_ extensions` using the command:

    ```
    jar -cvfm oracle.oaam.extensions.war oaam_
    extensions\META-INF\MANIFEST.MF -C oaam_extensions/ .
    ```

7.  Shut down the OAAM Admin and OAAM Server managed servers.

8.  Start the WebLogic Server where Oracle Adaptive Access Manager is deployed and log in to the WebLogic Administration Console.

9.  Navigate to Domain **Environment**, and select **Deployments** and lock the console.

10. Click **Install**.

11. Browse to the location of the `oracle.oaam.extensions.war`  file and select it by clicking the radio button next to the WAR file and clicking **Next**.

12. Ensure **Install this deployment as a library** is selected and click **Next**.

13. Select deployment targets, OAAM Admin and OAAM Server.

14. Click **Next** again to accept the defaults in this next page and then click **Finish**.

**15.** Click **Save** and then **Activate Changes**.

**16.** Start the OAAM Admin and OAAM managed servers.

### 9.9.2.1 Term and Condition Definitions

To configure terms and conditions check boxes and fields in the OTP registration page, add the properties in the sections following.

*Table 9–12    Terms and Conditions Checkbox*

| Property | Default Value | Description |
| --- | --- | --- |
| bharosa.uio.default.userinfo.inputs.enum.terms | 4 | Terms and Conditions enum value |
| bharosa.uio.default.userinfo.inputs.enum.terms.name | Terms and Conditions | Name for Terms and Conditions checkbox |
| bharosa.uio.default.userinfo.inputs.enum.terms.description | Terms and Conditions | Description for Terms and Conditions checkbox |
| bharosa.uio.default.userinfo.inputs.enum.terms.inputname | terms | HTML input name for Terms and Conditions checkbox |
| bharosa.uio.default.userinfo.inputs.enum.terms.inputtype | checkbox | HTML input type for Terms and Conditions checkbox |
| bharosa.uio.default.userinfo.inputs.enum.terms.values | true | Required values for Term and Conditions checkbox during registration and user preferences |
| bharosa.uio.default.userinfo.inputs.enum.terms.maxlength | 40 | HTML input max length for Terms and Conditions checkbox |
| bharosa.uio.default.userinfo.inputs.enum.terms.required | true | Required flag for Term and Conditions checkbox during registration and user preferences |
| bharosa.uio.default.userinfo.inputs.enum.terms.order | 5 | Order on the page for Terms and Conditions checkbox |
| bharosa.uio.default.userinfo.inputs.enum.terms.enabled | true | Enabled flag for Terms and Conditions enum item |
| bharosa.uio.default.userinfo.inputs.enum.terms.regex | .+ | Regular expression for validation of Terms and Conditions checkbox |
| bharosa.uio.default.userinfo.inputs.enum.terms.errorCode | otp.invalid.terms | Error code to get error message from if validation of Terms and Conditions fails |
| bharosa.uio.default.userinfo.inputs.enum.terms.managerClass | com.bharosa.uio.manager. user.DefaultContactInfoMa nager | Java class to use to save / retrieve Terms and Conditions from data storage |

## 9.9.3 Configuring Text and Fields on Registration and Preference Pages

Set up text and fields on registration and preference pages. Input properties includes maximum length for the email address the user can enter, validation for the email address field (expression), and so on.

**Mobile Input Registration Fields**

Mobile registration field definitions and validations for the OTP registration page are shown below.

These properties should be added to oaam_custom.properties.

*Table 9–13    Mobile Input Registration Fields*

| Property | Default Value | Description |
|---|---|---|
| bharosa.uio.default.userinfo.inputs.enum.mobile | 0 | Mobile phone enum value |
| bharosa.uio.default.userinfo.inputs.enum.mobile.name | Mobile Phone | Name for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile.description | Mobile Phone | Description for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile.inputname | cell number | HTML input name for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile.inputtype | text | HTML input type for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile.maxlength | 15 | HTML input max length for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile.required | true | Required flag for mobile phone field during registration and user preferences |
| bharosa.uio.default.userinfo.inputs.enum.mobile.order | 1 | Order on the page for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile.enabled | true | Enabled flag for mobile phone enum item |
| bharosa.uio.default.userinfo.inputs.enum.mobile.regex | \\D?(\\d{3})\\D?\\D?(\\d{3})\\D?(\\d{4}) | Regular expression for validation of mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile.errorCode | otp.invalid.mobile | Error code to get error message from if validation of mobile phone entry fails |
| bharosa.uio.default.userinfo.inputs.enum.mobile.managerClass | com.bharosa.uio.manager.user.DefaultContactInfoManager | Java class to use to save / retrieve mobile phone from data storage |

### Second Mobile Device Input Registration Field Properties Example

The following properties illustrate how to configure registration fields for a second mobile device on the OTP registration page.

*Table 9–14    Mobile Input*

| Property | Default Value | Description |
|---|---|---|
| bharosa.uio.default.userinfo.inputs.enum.mobile2 | 2 | Mobile phone enum value |
| bharosa.uio.default.userinfo.inputs.enum.mobile2.name | Mobile Phone 2 | Name for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile2.description | Mobile Phone 2 | Description for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile2.inputname | cell number 2 | HTML input name for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile2.inputtype | text | HTML input type for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile2.maxlength | 15 | HTML input max length for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile2.required | true | Required flag for mobile phone field during registration and user preferences |
| bharosa.uio.default.userinfo.inputs.enum.mobile2.order | 2 | Order on the page for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile2.enabled | true | Enabled flag for mobile phone enum item |

*Table 9–14 (Cont.) Mobile Input*

| Property | Default Value | Description |
|---|---|---|
| bharosa.uio.default.userinfo.inputs.enum.mobile2.regex | \\D?(\\d{3})\\D?\\D ?(\\d{3})\\D?(\\d{4}) | Regular expression for validation of mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile2.errorCode | otp.invalid.mobile | Error code to get error message from if validation of mobile phone entry fails |
| bharosa.uio.default.userinfo.inputs.enum.mobile2.managerClass | com.bharosa.uio.mana ger.user.DefaultContac tInfoManager | Java class to use to save / retrieve mobile phone from data storage |

### Email Address Input Registration Field Properties

Add these properties to configure the email address registration fields on the OTP registration page.

*Table 9–15 Email Input*

| Property | Default Value | Description |
|---|---|---|
| bharosa.uio.default.userinfo.inputs.enum.email | 1 | Email address enum value |
| bharosa.uio.default.userinfo.inputs.enum.email.name | Email Address | Name for email address field |
| bharosa.uio.default.userinfo.inputs.enum.email.description | Email Address | Description for email address field |
| bharosa.uio.default.userinfo.inputs.enum.email.inputname | email | HTML input name for email address field |
| bharosa.uio.default.userinfo.inputs.enum.email.inputtype | text | HTML input type for email address field |
| bharosa.uio.default.userinfo.inputs.enum.email.maxlength | 40 | HTML input max length for email address field |
| bharosa.uio.default.userinfo.inputs.enum.email.required | true | Required flag for email address field during registration and user preferences |
| bharosa.uio.default.userinfo.inputs.enum.email.order | 2 | Order on the page for email address field |
| bharosa.uio.default.userinfo.inputs.enum.email.enabled | false | Enabled flag for email address enum item |
| bharosa.uio.default.userinfo.inputs.enum.email.regex | .+@[a-zA-Z_ ]+?\\.[a-zA-Z]{2,3} | Regular expression for validation of email address field |
| bharosa.uio.default.userinfo.inputs.enum.email.errorCode | otp.invalid.email | Error code to get error message from if validation of email address entry fails |
| bharosa.uio.default.userinfo.inputs.enum.email.managerClass | com.bharosa.uio.ma nager.user.DefaultC ontactInfoManager | Java class to use to save / retrieve email address from data storage |

### Second Email Address Input Registration Field Properties Example

The following properties illustrate how to configure registration fields for a second email address on the OTP registration page.

*Table 9–16 Email Input*

| Property | Default Value | Description |
|---|---|---|
| bharosa.uio.default.userinfo.inputs.enum.email2 | 2 | Email address enum value |
| bharosa.uio.default.userinfo.inputs.enum.email2.name | Email Address 2 | Name for email address field |
| bharosa.uio.default.userinfo.inputs.enum.email2.description | Email Address 2 | Description for email address field |
| bharosa.uio.default.userinfo.inputs.enum.email2.inputname | email2 | HTML input name for email address field |

*Table 9–16   (Cont.)  Email Input*

| Property | Default Value | Description |
| --- | --- | --- |
| bharosa.uio.default.userinfo.inputs.enum.email2.inputtype | text | HTML input type for email address field |
| bharosa.uio.default.userinfo.inputs.enum.email2.maxlength | 40 | HTML input max length for email address field |
| bharosa.uio.default.userinfo.inputs.enum.email2.required | true | Required flag for email address field during registration and user preferences |
| bharosa.uio.default.userinfo.inputs.enum.email2.order | 2 | Order on the page for email address field |
| bharosa.uio.default.userinfo.inputs.enum.email2.enabled | false | Enabled flag for email address enum item |
| bharosa.uio.default.userinfo.inputs.enum.email2.regex | .+@[a-zA-Z_ ]+?\\.[a-zA-Z]{2,3} | Regular expression for validation of email address field |
| bharosa.uio.default.userinfo.inputs.enum.email2.errorCode | otp.invalid.email | Error code to get error message from if validation of email address entry fails |
| bharosa.uio.default.userinfo.inputs.enum.email2.managerClass | com.bharosa.uio.manager.user.DefaultContactInfoManager | Java class to use to save / retrieve email address from data storage |

## 9.10  Configuring OTP Presentation

By default, challenge devices are configured through rules. The rules are under the Authentipad checkpoint and determine the type of device to use based on the purpose of the device (ChallengeEmail, ChallengeSMS, ChallengeQuestion, and so on).

To change the OTP Device used for challenges, change the OTP challenge type for the rule's result action.

Alternatively, if you want to configure challenge devices using properties you can bypass the Authentication Pad checkpoint by following these instructions:

1. Log in to OAAM Admin.

2. In the Navigation tree, double-click **Properties** under the **Environment** node. The **Properties Search** page is displayed.

3. Set `bharosa.uio.default.use.authentipad.checkpoint` to `false`.

4. Edit `bharosa.uio.default.<ChallengeType>.authenticator.device=<Device>` with the challenge type and the property for the desired device.

   ```
   bharosa.uio.default.ChallengeSMS.authenticator.device=DeviceTextPad
   bharosa.uio.default.ChallengeEmail.authenticator.device=DeviceTextPad
   ```

   Table 9–17 shows the property and the authentication pad that would be used. In the above example, the SMS authenticator is the Text Pad since the property, DeviceTextPad, was specified. (DeviceKeyPadAlpha would display a alphanumeric KeyPad.)

For authentication device types, refer to Table 9–17.

*Table 9–17    Authentication Device Type*

| Property | Description |
| --- | --- |
| None | No HTML page or authentication pad |
| DeviceKeyPadFull | Challenge user using KeyPad. |
| DeviceKeyPadAlpha | Challenge user with the alphanumeric KeyPad (numbers and letters only, no special characters) |
| DeviceTextPad | Challenge user using TextPad. |
| DeviceQuestionPad | Challenge user using QuestionPad. |
| DevicePinPad | Challenge user using PinPad. |
| DeviceHTMLControl | Challenge user using HTML page instead of an authentication pad. |

The OTP device is displayed at the next log in to the application.

## 9.11  Configuring Failure Counter

When a user fails the OTP challenge, a counter is updated to indicate that user has had a failure. The failure counter looks across sessions.

The failure counter is set by default in the OAAM Challenge Policy, but you can customize it by following these instructions:

1. Open the OAAM Challenge Policy.

2. Open the appropriate maximum failed OTP rule.

3. In the Conditions tab, select `User: Check OTP failures`.

4. Edit the appropriate properties.

*Table 9–18    User: Check OTP failures Values*

| Property | Description |
| --- | --- |
| Description | Checks if user's OTP failure counter value is over a specified value. |
| Failures more than or equal to | The number of failed attempts allowed |
| If above or equal, return | True or False |
| OTP Challenge Type | The challenge type is the channel that OTP is using to challenge the user. |

## 9.12  Customizing OTP Registration and Messaging

The registration page could be fully customized using the resource bundle (client_resource_<locale>.properties file). Also, the challenge type message subject, the body of the message, and the message itself could be fully customized by specifying the custom values in resource bundle files and deploying the changes via OAAM extension shared libraries.

### 9.12.1  Customizing Terms and Conditions

To customize the Terms and Condition text, add the following properties to the resource bundle, client_resource_<locale>.properties:

*Table 9–19    Messaging of Terms and Conditions*

| Property | Descriptions |
| --- | --- |
| bharosa.uio.default.userinfo.inputs.enum.terms.name | I agree to the [ENTER COMPANY OR SERVICE NAME HERE] terms & conditions. Click to view full <a href="javascript:infoWindow('terms');">Terms & Conditions</a> and <a href="javascript:infoWindow('privacy');">Privacy Policy</a>. |
| bharosa.uio.default.userinfo.inputs.enum.terms.description | Message and Data Rates May Apply. <br/>For help or information on this program send "HELP" to [ENTER SHORT/LONG CODE HERE]. <br/>To cancel your plan, send "STOP" to [ENTER SHORT/LONG CODE HERE] at anytime.<br/><br/>For additional information on this service please go to <a href="" target="_blank">[ENTER INFORMATIONAL URL HERE]</a>.<br/><br/><b>Supported Carriers:</b><br/>AT&T, Sprint, Nextel, Boost, Verizon Wireless, U.S. Cellular&reg;, T-Mobile&reg;, Cellular One Dobson, Cincinnati Bell, Alltel, Virgin Mobile USA, Cellular South, Unicel, Centennial and Ntelos |

The value for `bharosa.uio.default.userinfo.inputs.enum.terms.name` includes placeholder links that use OAAM Server popup messaging for "Terms & Conditions" and "Privacy Policy". The property and resource keys for the contents of the popups are listed as follows.

*Table 9–20    Terms & Conditions and Privacy Policy Popup Messaging*

| Property | Descriptions |
| --- | --- |
| bharosa.uio.default.messages.enum.terms.name | Terms and Conditions |
| bharosa.uio.default.messages.enum.terms.description | PLACEHOLDER TEXT FOR TERMS AND CONDITIONS |
| bharosa.uio.default.messages.enum.privacy.name | Privacy Policy |
| bharosa.uio.default.messages.enum.privacy.description | PLACEHOLDER TEXT FOR PRIVACY POLICY |

## 9.12.2  Customizing Mobile Input Registration Fields

To customize mobile input fields, these properties can be added to the resource bundle, client_resource_<locale>.properties:

*Table 9–21    Mobile Input - Resource Bundle*

| Property | Default Value | Description |
| --- | --- | --- |
| bharosa.uio.default.userinfo.inputs.enum.mobile.name | Mobile Phone | Name for mobile phone field |
| bharosa.uio.default.userinfo.inputs.enum.mobile.description | Mobile Phone | Description for mobile phone field |

## 9.12.3  Customizing Registration Page Messaging

To customize the registration page messaging, add the following registration properties to client_resource_<locale>.properties:

*Table 9–22    Registration Resource Bundle*

| Property | Default Value |
| --- | --- |
| bharosa.uio.default.register.userinfo.title | OTP Anywhere Registration |
| bharosa.uio.default.register.userinfo.message | For your protection please enter your mobile telephone number so we may use it to verify your identity in the future. Please ensure that you have text messaging enabled on your phone. |
| bharosa.uio.default.register.userinfo.registerdevice.message | Check to register the device that you are currently using as a safe device: |
| bharosa.uio.default.register.userinfo.continue.button | Continue |
| bharosa.uio.default.register.userinfo.decline.message | If you decline you will not be asked to register again. |
| bharosa.uio.default.register.userinfo.decline.button | Decline |

### 9.12.4  Customizing Challenge Messaging

To customize the challenge type fields, add the following properties to the resource bundle, client_resource_<locale>.properties:

*Table 9–23    Challenge Type Resource Bundle Items*

| Property | Default Value |
| --- | --- |
| bharosa.uio.default.ChallengeSMS.message | For your protection please enter the code we just sent to your mobile telephone. If you did not receive a code please ensure that text messaging is enabled on your phone and click the resend link below. |
| bharosa.uio.default.ChallengeSMS.registerdevice.message | Check to register the device that you are currently using as a safe device: |
| bharosa.uio.default.ChallengeSMS.continue.button | Continue |

### 9.12.5  Customizing the OTP Messaging

To customize the OTP messaging, add these properties to the resource bundle, client_resource_<locale>.properties:

> **Note:**   User facing strings need to be duplicated into resource bundle. Resource bundle values can be customized by adding them to the `client_resource_<locale>.properties` and deploying the file in OAAM Extensions Shared Library.

*Table 9–24    Challenge Type Resource Bundle Items*

| Property | Default Value |
| --- | --- |
| bharosa.uio.default.ChallengeSMS.incorrect.message | Incorrect OTP. Please try again. |
| bharosa.uio.default.ChallengeSMS.message.subject | Oracle OTP Code |
| bharosa.uio.default.ChallengeSMS.message.body | Your Oracle SMS OTP Code is: {0} |

## 9.13  Customizing One-Time Password Generation

You can configure the one-time password through properties edits. The following properties are used to generate the OTP:

```
# OTP pin generation config
bharosa.uio.default.otp.generate.code.length = 5
bharosa.uio.default.otp.generate.code.characters = 1234567890
```

The default OTP codes will be 5 characters made up of the numbers 0-9 (for example: 44569).

`bharosa.uio.default.otp.generate.code.length` designates the length of the OTP.

`bharosa.uio.default.otp.generate.code.characters` designates the characters to use when generating the OTP.

An example is shown below for generating a 4 character OTP code with numbers 0-9 and letters a-d (for example: 0c6a):

```
bharosa.uio.default.otp.generate.code.length = 4
bharosa.uio.default.otp.generate.code.characters = 1234567890abcd
```

## 9.14 Customizing One Time Password Expiry Time

> **Note:** This property works for the OTP API, but as of now OAAM Server does not use the API. Hence, by default, OAAM Server OTP is valid for the session or until used.

To set up OTP SMS password expiry time, add the following property:

`bharosa.uio.default.challenge.type.enum.ChallengeSMS.otpexpirytimeMs`

To set up OTP e-mail password expiry time, add the following property:

`bharosa.uio.default.challenge.type.enum.ChallengeEmail.otpexpirytimeMs` to `oaam_custom.properties`.

The time is in milliseconds. If the value is not in milliseconds, you will have to perform a conversion. For example, if you want to set the expiration time for OTP to be 5 minutes, then you must set the property to 300000 ms (5 minutes).

# Part IV

## Managing Policy Configuration

This part contains information about managing policy configurations in Oracle Adaptive Access Manager 11*g*.

It contains the following chapters:

# 10

# Managing Policies, Rules, and Conditions

Policies are used by organizations to monitor and manage fraud or to evaluate business elements. Policies contain security rules and configurations used to evaluate the level of risk at each checkpoint.

This chapter introduces you to the concepts behind policies, rules and conditions and provides information about creating and managing them.

## 10.1 Introduction to Policies, Rules, and Conditions

This section introduces you to the concept of policies and rules and how they are used in Oracle Adaptive Access Manager.

### 10.1.1 Policies

A policy is a collection of rules associated with a checkpoint. The outcome of the policy evaluation is a score, actions and alerts. The policy outcomes can be used to enforce decisions by client applications. For information on rules, see Section 10.1.2, "Rules."

Using Oracle Adaptive Access Manager, you can create policies based on your business requirements. The attributes/datapoints of the activities you are interested in are mapped to conditions and the evaluations to perform are translated into rules. These rules are added to a policy. Checkpoints are set up in the session for when the policy evaluates the activity. For example, a policy can be executed during the Pre-Authentication checkpoint. The Pre-Authentication checkpoint is a point in time before the user enters the password. When the rules are run, data is collected. For information, see Section 10.1.4, "Checkpoints."

During the normal course of business, the system looks for datapoints the conditions were mapped to. When all the conditions met, the system calculates a score, and depending on the policy that you defined earlier for handling the situation, it may generate alerts in real-time, or trigger actions, or both. For example, outcomes can be challenging or blocking the user or activating an alert.

A rule evaluates to true when all the conditions match. The outcome of a rule is a score and optionally actions or alerts, or answers and alerts. The outcome of a policy is decided by applying a scoring policy on the rule scores of the policy. In addition to the score, you can optionally configure trigger combinations which are combinations of rule results of the policy and that can invoke actions and/or generate alerts. For more information about trigger combinations, see Section 10.1.10, "Trigger Combinations and Triggers."

Because fraud or the business climate is ever-changing, you must re-evaluate policies periodically to reflect new situations and use Oracle Adaptive Access Manager to update and keep them current.

**Policy Structure**

illustrates the policy structure.

*Figure 10–1   Policy Structure*
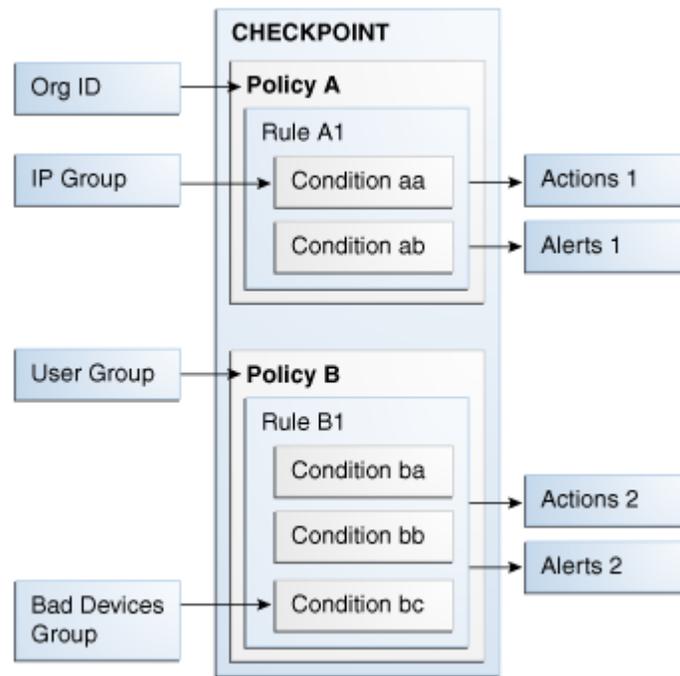


A checkpoint is when a policy is called to run its rules.

Rules contain configurable evaluator statements called conditions.

Policies are scoped by linking them to user groups and Organization IDs.

Actions, alerts, IP, device, and other groups are associated with conditions, trigger combinations, and checkpoint overrides.

## 10.1.2  Rules

A rule is a collection of conditions. Exceptions can be specified using preconditions. A rule evaluates the conditions and the outcomes of rules are alerts, an action, and a score. The rule is evaluated to "true" when all preconditions are met and all conditions evaluate to "true." When a rule is evaluated to "true", specified alerts are created and the associated actions and score are given to the policy for further evaluation.

## 10.1.3  Conditions

Conditions are configurable evaluation statements used in the evaluation of historical and runtime data. Conditions use data-points (session and/or historical) to evaluate risk or business logic. They are grouped based on the type of data used in the condition. For example, user, device, and location.

Conditions are pre-packaged in the system and cannot be created by a user.

Rules are made up of conditions. Conditions may take user inputs when adding them to a rule. Conditions can evaluate to true or false based on the available data. When multiple conditions are added, the conjunction between the conditions is always AND.

Refer to the example in Table 10–1.

*Table 10–1    Multiple Conditions*

| Condition 1 | Condition 2 | Rule Result |
|---|---|---|
| True | True | True |
| False | False | False - Rule is not triggered |
| True | False | False |
| False | True | False |

For information on the conditions available in the system, see Appendix C, "Conditions Reference."

## 10.1.4  Checkpoints

The checkpoint is a decision and enforcement point when policies are call to run their rules. All policies configured for a checkpoint are evaluated and the outcome is a score and an action or both.

OAAM Server uses out-of-the-box policies and checkpoints to control the user flow. API-based integrations can create new checkpoints, configure policies, and drive the flow.

### Checkpoint Example

A fraudster has stolen a user's user name and password and wants to perform a wire transfer. To accomplish the goal of performing a wire transfer, the fraudster must pass through multiple security gates. The fraudster is caught during Post-Authentication. For example, if the fraudster is using an anonomyzing proxy to mask the location, a challenge might occur during Post-Authentication. When the fraudster fails to provide the correct answers, fraud is prevented.

## 10.1.5  Groups

Groups are like items that have been gathered together to simplify configuration workloads. Grouping enables you to view and administer the collection of like items as a single group instead of administering the individual members of a group. The types of groups you can create include User ID, User Name, Location, Device, Action, and Alert.

## 10.1.6  Actions and Action Groups

Actions are used to control the application flow.

An action is an event activated when a rule is triggered. For example: block access, challenge question, ask for PIN or password, and so on. An action can be also activated based on a score for particular checkpoint.

The client applications like OAAM Server or the native integrated client influence the resultant out-of-the-box actions. Users may also create custom actions that are used by their applications.

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

For information on action groups, see Chapter 12, "Managing Groups."

### 10.1.7 Alerts and Alert Groups

Alerts are messages that indicate the occurrence of an event. An event can be that a rule was triggered, a trigger combination was met or an override was used.

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

For information on creating an alert, see Chapter 12, "Managing Groups."

### 10.1.8 User Group Linking

In Group Linking, the Run mode can be specified to execute policies for all users or selected user groups.

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

The "Linked Users" option links a policy to a User ID group or several User ID groups.

The "All Users" option links a policy to all users. If group linking shows "All Users," all the available linking is ignored. If a user selects group linking as "All Users," the link option would be disabled.

### 10.1.9 Run Mode

Run mode is either "All Users" or "Linked Users." It determines if a policy is evaluated for all users or for the user groups linked to that policy. If a policy is being evaluated as a nested policy then the run mode is ignored.

### 10.1.10 Trigger Combinations and Triggers

Trigger combinations are additional results and policy evaluation that are generated if a specific sequence of rules trigger.

Trigger combinations can be used to override the outcome of rules. Each trigger combination can specify alerts, actions and either a score or another policy to run. Trigger combinations evaluate sequentially, stopping as soon as a rule return combination is matched. Alerts are added to any actions and alerts triggered by individual rules. Action group replace the actions returned by the individual rules.

When a trigger combination triggers another policy, that policy is said to be nested within the policy. A policy can be nested within other policies and also can be evaluated on its own.

For information on trigger combinations, see Section 10.13, "Working with Trigger Combinations."

For an example of setting up a trigger combination, see Section 10.34.7, "Use Case: Trigger Combination."

### 10.1.11 Nested Policies

A nested policy is a secondary policy used to further quantify the risk score in instances where the original result output by the system is inconclusive. Nested policies can be assigned to ensure a higher degree of accuracy for the risk score.

A nested policy in a trigger combination is executed only when a specific sequence of rule results is sent from the primary policy. Nested policies therefore reduce false positives and negatives.

### 10.1.12 Evaluating a Policy within a Rule

Oracle Adaptive Access Manager can evaluate another policy as part of a rule by using the "System: Evaluation Policy" condition. The result of the evaluated policy is propagated. This is called a "condition execution."

### 10.1.13 Scores and Weight

The score is a number configured by the user that is assigned to a rule when the rule evaluates to true. The user can configure a scoring policy that is used to combine the scores of the rules in a policy and assign a score to the policy. The scores from various policies are combined using a policy set level scoring policy.

Weight is the multiplier values used on policies scores to influence the total score.

For more information on scores and weights and how they are used in risk assessment, see Chapter 14, "Using the Scoring Engine."

### 10.1.14 Scoring Engine

A scoring engine is provided at the policy level and at the checkpoint level.

The policy scoring engine is applied to rule scores to determine the risk for each policy.

The policy set scoring engine is applied to the scores of the policies under a checkpoint to determines the score for the checkpoint. The default scoring engine at the checkpoint level is "Maximum."

For more information on the scoring engine, see Chapter 14, "Using the Scoring Engine."

### 10.1.15 Import Policies

The policy is added to the system or it overwrites/updates an existing policy depending on whether the same policy name exists. If the name already exists, the policy is updated. If the name does not exist, the imported policy is added to the system.

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

### 10.1.16 Policy Type

The concept of policy type has been removed from the product.

Only security policies are available in 11*g*. Although policy types for the 10*g* policies are retained in the OAAM database, OAAM 11*g* ignores the policy types of Business, Third-party, and Workflow in the database and treats all policy types as "Security" policies for all purposes.

Since there are no policy types, the policy type scoring engine is ignored and the scoring engine at the checkpoint level is applied for all policies.

### 10.1.17 Failure Counters

When a user fails a challenge, a counter is updated to indicate that user has had a failure. The failure counter looks across sessions. When a user has a maximum of three failures, he is locked from this type of challenge. For example, he could be OTP locked.

## 10.2 Planning Policies

Read the following section to help you in planning your policy.

**Rule Conditions**

Oracle Adaptive Access Manager has a library of conditions used to configure rules.

To use these conditions, import them into your system by following the instructions in Section 10.26, "Importing Conditions."

**Planning New Policies**

If you have created policies, use this chapter effectively in any order that is convenient for you.

If you want to start creating policies for your system, follow this outline:

1. As you begin formulating a policy, gather intelligence from various sources to identify needs and develop requirements to address them.

   For example, you can run reports to identify security trends that need to be addressed.

2. Given the results, develop requirements to address needs.

   - Use cases

   - Rule conditions

   - Expected outcomes (action, alerts, and scores)

   - Applications involved

   - User groups involved

3. Decide which type of scoring engine to apply.

   For information on scoring engines, see Chapter 14, "Using the Scoring Engine."

4. Plan policies based on requirements.

   - Datapoints to profile

   - Rules for use cases

   - Thresholds defined by rules

   - Outcomes needed - scores, actions, and alerts

   - Exclusion groups

   For information on rule modeling, see Appendix E, "The Discovery and OAAM Policy Development Processes."

5. Build alert and action groups so that they are available when you build the policy.

   For information, see Section 12.10, "Creating a Group."

6. Create the policy.

   For information, see Section 10.8, "Creating Policies."

## 10.3  Overview of Creating a Policy

This section presents an overview of creating a policy.

To create a policy, the general steps are:

1. Search for the policy to see if the policy exists.

2. View policy details to see if the rule you need is available in the policy.

3. Create a policy with the appropriate name (for example, Block-From-BlackList), type and assign the relevant checkpoint, scoring and weight.

   For more information on assigning scores and weight, see Chapter 14, "Using the Scoring Engine."

4. Add the required rules with the conditions to the policy and use trigger combinations to determine the order of rule to be triggered.

   The new rules evaluate and handle patterns or practices, or specific activities that you may run across in the day-to-day operation of your business.

   There are two ways to add rules to a policy:

   - Create rules to add to the policy, or

   - Copy rules to the policy

5. Link the policy to the user group as appropriate.

   The policy and rules execute for the user group.

*Figure 10–2   Overview of Creating a Policy*
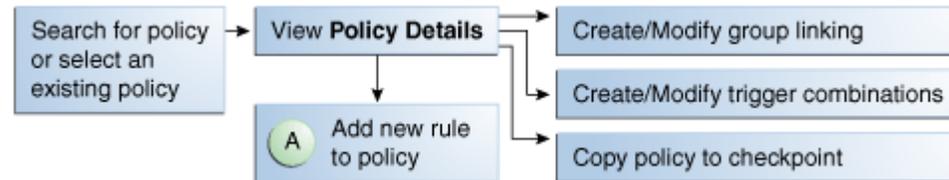


To create a new rule to add to a policy:

1. Specify the preconditions

2. Add conditions

3. Reorder conditions/modify parameters

4. Specify result values

*Figure 10–3   Overview of Adding a New Rule*
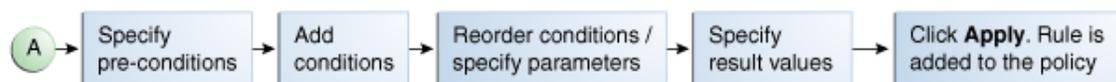


## 10.4  Navigating to the Policies Search Page

To open the **Policies Search** page, in the Navigation tree, double-click **Policies**. The **Policies Search** page is displayed.

Alternatively, you can open the **Policies Search** page by:

- Right-clicking **Policies** in the Navigation tree and selecting **List Policies** from the context menu.

- Selecting **Policies** in the Navigation tree and then choosing **List Policies** from the **Actions** menu.

- Clicking the **List Policies** button in the Navigation tree toolbar.

The **Policies Search** page is the starting place for managing your policies. It is also the home page for the Security Administrator.

From the **Policies Search** page, you can:

- Search for a policy

- View a list of policies

- Create a new policy

- Import a policy

- Export policies

- Export policies and create a delete script

- Delete policies

- Navigate to the **Policy Details** page

An example of a **Policies Search** page is shown in Figure 10–4, "Policies Search Page".

*Figure 10–4   Policies Search Page*



## 10.5  Searching for a Policy

In the **Policies Search** page, you search for a policy by specifying criteria in the Search filter.

When the **Policies Search** page first appears, the **Search Results** table is empty. You must press **Search** to see a list of policies in the Oracle Adaptive Access Manager environment.

To search for policies:

1. In the Navigation tree, double-click **Policies**. The **Policies Search** page is displayed.

2. Specify criteria in the Search Filter to locate the policy and click **Search**.

   Clicking **Reset** instead of **Search** resets the search criteria.

   The search filter criteria are described in Table 10–2.

*Table 10–2    Policies Search Filter Criteria*

| Filters and Fields | Descriptions |
|---|---|
| Linked Groups | Users can filter policies based on the user groups they are linked with. |
| | The Linked Groups filter is disabled when the Run Mode is "Not Linked" since there are no associated User ID groups. |
| Policy Name | Name of the policy. You can enter the complete name or part of a policy name. For example, if you enter HTTP, any policy with HTTP in any part of its name will appear. |
| Policy Status | Status of the policy: Active or Disabled. |
| | Defines the state of the object or its availability for business processes. |
| | For information, refer to **Policy Status**. |
| Checkpoints | Point during the session the rules in a policy are evaluated. |
| Run Mode | Run mode enables you to select whether to link the policy to all users, a specified User ID group, or not to link the policy. Linking a policy to a group enables the policy to execute/run for the set of users within the linked group. |
| | ■ The "All Users" option links a policy to all users. The policy is targeted for all users. |
| | ■ The "Linked Users" option links a policy to a User ID group or several User ID groups. The policy is targeted to a specified set of users. |
| Created Date | Time when policy was created. |
| Update Time | Time when policy was last updated. |

## 10.6  Viewing a Policy or a List of Policies

Depending on the search performed, a policy or a list of policies is displayed in the Search Results table. The policies that are displayed from a search are those that match the criteria specified in the **Linked Groups**, **Policy Name**, **Policy Status**, **Checkpoint**, and **Run Mode** fields.

You can sort the **Search Results** table by sorting on a column.

Each policy has a name. If the description is too long to be fully shown, you can place the mouse over the text to see the entire description.

The **Search Results** table provides quick access to the **Policy Details** page for a policy. Click the policy name for the policy you are interested in to view more details.

## 10.7  Viewing Policy Details

By clicking the policy name, the **Policy Details** page for the specific policy is displayed.

The **Policy Details** page enables you to view and edit the details of a policy. You can also access the **Policy Details** page through the Policy Tree. For information, refer to Chapter 3, "Oracle Adaptive Access Manager Navigation."

The Policy Details page provides the following four tabs:

■ **Summary** - Enables you to view and edit the general details of the policy

■ **Rules** - Enables you to view a list of all the rules of the policy, and add and delete them.

■ **Trigger Combinations** - Enables you to view the trigger combinations of the policy and to add, delete, and to edit them.

- **Group Linking** - Enables you to link a policy to a User ID group

The number of rules, trigger combinations, and group links present in the policy is shown in parenthesis on the **Policy Details** page tabs. Disabled rules are also included in the count.

## 10.8 Creating Policies

A policy is a collection of rules and configured to evaluate and handle patterns or practices, or specific activities that you may run across in the day-to-day operation of your business.

For a new policy to function, you must create the policy and then perform edits to the policy.

To create a new policy:

1. In the Navigation tree, double-click **Policies**. The **Policies Search** page is displayed.

2. From the **Policies Search** page, click the **New Policy** button.

   The **New Policy** page is displayed where you can specify details to create a new policy.

   Alternatively, you can open a **New Policy** page by:

   - Right-clicking **Policies** in the Navigation tree and selecting **New Policy** from the context menu.

   - Selecting **Policies** in the Navigation tree and then choosing **New Policy** from the **Actions** menu.

   - Clicking the **Create new Policy** button in the Navigation tree toolbar.

   - Selecting the **Create New Policy** button from the **Search Results** toolbar.

   - Selecting **New Policy** from the **Actions** menu in **Search Results**.

   All fields in the **Summary** tab are pre-populated except **Name** and **Description**.

   When the **New Policy** page first appears, the default values for the new policy are as follows:

   - **Policy Status**: Active

   - **Checkpoint**: Pre-Authentication

   - **Scoring Engine**: Average

   - **Weight**: 100

   After you create a new policy, you can add rules, trigger combinations, and user groups.

*Figure 10–5   New Policy*



3. In the **Summary** tab, in the **Policy Name** box, type the name of the new policy.

   Enter between 1 and 255 characters for the policy name and for the description.

4. If you want the policy to be enabled as soon as it is created, keep the default, **Active**, for the **Policy Status**.

   If you want to policy to be disabled, select **Disabled**.

   A policy that is disabled is not enforced at the checkpoint.

   Disabling a policy does not remove it from the system. You are able to enable the policy at a later date.

5. From the **Checkpoint** list, select the point before and during the session when you want the policy to be executed.

   For example, if you want to initiate an action after successful authentication select post-authentication as a checkpoint.

   For more information on checkpoints, see Section 10.1.4, "Checkpoints."

6. From the **Scoring Engine** list, select the fraud analytic engine you want to use to calculate the numeric score that determines the risk level.

For more information on the Scoring Engine, see Chapter 14, "Using the Scoring Engine."

**7.** From the **Weight** list, enter a value from 0 to 100 as the multiplier if you want to use a weighted scoring engine to influence the total score.

If the policy uses a "weighted" scoring engine, both score and weight (multiplier value) are used to influence the total score calculations. If the policy is not using a "weighted" scoring engine, only the score is used to influence the total score.

**8.** Enter a description for the policy in the **Description** box.

**9.** Click **Apply** to create the policy.

A confirmation dialog appears with a message that the policy was created successfully.

**10.** Click **OK** to dismiss the confirmation dialog.

The **Rules**, **Trigger Combinations**, and **Group Linking** tabs are enabled after you click **OK**.

The **Copy Policy** button is enabled if you want to copy the policy to another checkpoint. For details, see Section 10.16, "Copying a Policy to Another Checkpoint."

To edit the policy so that it functions:

**1.** When the policy is created, you can add a rule to the policy by creating a new rule within a policy (Section 10.12, "Adding a New Rule").

When you add a rule, you can specify:

- **Preconditions**. For information, see Section 10.21.2, "Specifying Preconditions."

- **Conditions**. For information, see Section 10.27, "Adding Conditions to a Rule."

- Order of conditions/parameter values

- **Results**. For information, see Section 10.21.3, "Specifying the Results for a Rule."

**2.** Then, you must link the policy to a group of type, User ID, or all users in order for the policy to execute. Group linking enables the policy to execute/run for that set of users or all users. For information, see Section 10.9, "Linking Policy to All Users or a User ID Group."

**3.** Configure trigger combinations if you want to specify outcomes different from the ones for the individual rules. For information, see Section 10.13, "Working with Trigger Combinations."

## 10.9 Linking Policy to All Users or a User ID Group

Group linking enables you to specify the users that a policy links to. You must link the policy to a group in order for the policy to function.

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

The **All Users** option links a policy to all users. If group linking shows **All Users**, all the available linking is ignored. If a user selects group linking as **All Users**, the link option would be disabled.

The total number of groups linked in the policy appears in parenthesis next to the Group Linking tab title.

### 10.9.1 Linking a Policy to a Group

After the policy is created, you can link the policy to a User ID group or several User ID groups, which enables the policy and rules to execute/run for that set of users.

1. Navigate to the **Policy Details** page.

   a. In the Navigation tree, select **Policies**. The **Policies Search** page is displayed.

   b. Search for the policy that you want.

   c. Click the policy name to open its **Policy Details** page.

2. From the **Policy Details** page, click the **Group Linking** tab.

3. For **Run Mode**, specify **Linked Users**.

4. In the table header, click the **Link** icon.



   The **Link Group** screen appears where you can enter details to link a group to the policy.

5. The available target sets appear in the associated box.

   From the **Group Name** list, select the group you want to link to the policy.

   Only user groups are listed.

   **Group Name** is a required field.

6. Enter linking notes.

7. Click **Link Group**.

## 10.10 Editing a Policy's General Information

To edit a policy's general information:

1. Search for the policy you are interested in, as described in Section 10.5, "Searching for a Policy."

2. In the **Search Results** table, click the name of the policy you want to edit.

   The **Summary** tab displays general details about the policy, as shown in Table 10–6, "Policy Details Summary Tab".

*Figure 10–6   Policy Details Summary Tab*



*Table 10–3    Policy Details Summary Tab*

| Field | Description |
| --- | --- |
| Policy Name | Name of the policy. |
| Policy Status | Status of the policy: Active or Disabled. |
| | Defines the state of the object or its availability for business processes. |
| | For information, refer to **Policy Status**. |
| Checkpoint | Point during the session the rules in a policy are evaluated. |
| Scoring Engine | Fraud analytic engine you want to use to calculate the numeric score that determines the risk level. |
| Weight | Multiplier used to influence the total score at various evaluation levels. Weight is an integer value from 0 to 100 |
| Description | Description for the policy. |

3. To edit the policy's general information, make the changes you want in the **Summary** tab and then click **Apply**.

The policy details are updated successfully.

## 10.11 Activate/Disable Policies

To activate/disable a policy:

1. Search for the policy you are interested in, as described in Section 10.5, "Searching for a Policy."

2. In the **Search Results** table, click the name of the policy you want to activate/disable.

3. Changes the policy status in the **Summary** tab and then click **Apply**.

   For information, refer to **Policy Status**.

## 10.12 Adding a New Rule

You can only create a rule from within a policy. The new rule cannot be saved until you add a condition to it.

Creating a rule involves the following steps:

- Starting the Rule Creation Process
- Specifying General Rule Information
- Configuring Preconditions
- Adding Conditions
- Specifying Results for the Rule
- Adding or Copying a Rule to a Policy

### 10.12.1 Starting the Rule Creation Process

To start the rule creation process:

1. In the Navigation tree, select **Policies**. The **Policies Search** page is displayed.

2. Search for the policy that you are interested in.

3. In the **Search Results** table, click the name of the policy. The **Policy Details** page for that policy is displayed.

4. In the **Policy Details** page, click the **Rules** tab.

5. In the **Rules** tab, click the **Add** button on the row header or select **New Rule** from the **Action** menu.

   The **New Rule** page is displayed.

*Figure 10–7 New Rule*



The next steps to the rule creation process are:

1. Specifying General Rule Information

2. Specifying Preconditions

3. Adding Conditions to a Rule

   a. Reorder conditions

   b. Modify parameters

4. Specifying the Results for a Rule

The **Rule Status** for new rules has the default value of Active.

## 10.12.2 Specifying General Rule Information

Table 10–4, " New Rule Page" summarizes the general information of a rule.

*Table 10–4    New Rule Page*

| Field | Description |
| --- | --- |
| Rule Name | Name of the rule. Enter between 1 and 4000 characters. |
| Policy Name | Name of the policy. (Read-only) |
| Rule Status | Status of the rule: Active or Disabled. If the rule status is changed from Active to Disabled, the rule is disabled and cannot be added to a policy. A policy that already contains the rule is not affected and continues to function as before. |
| Description | Description for the rule. Enter between 1 and 4000 characters. |

To add general information about the rule, the procedure is as follows:

1. In the **Summary** tab, enter the name of the rule and a description. Duplicate rule names are allowed across policies, but not within the same policy.

   If you try to navigate to one of the other tabs before entering a rule name or description, an error message reminds you that a value is required.

   The policy name cannot be changed.

2. If you want to disable the rule, select **Disabled**. **Rule Status** has the default value of **Active**. A rule that is disabled is not run when the policy is enforced.

## 10.12.3 Configuring Preconditions

To configure preconditions for the rule, follow the procedure in Section 10.21.2, "Specifying Preconditions."

Through preconditions, you can specify the group to exclude and the geolocation confidence factor parameters.

## 10.12.4 Adding Conditions

To add conditions for the rule, follow the procedure in Section 10.27, "Adding Conditions to a Rule."

## 10.12.5 Specifying Results for the Rule

To specify the results for if the rule triggers, follow the procedure in Section 10.21.3, "Specifying the Results for a Rule."

You can select from the following types of results:

- Score and Weight

- Actions

  An action is an event activated when a rule is triggered. For example: block access, challenge question, ask for PIN or password, and so on. For information about action groups, see Chapter 12, "Managing Groups."

- Alerts

  An alert is a message generated when a rule is triggered. For example: login attempt from a new country for this user. For information about alert groups, see Chapter 12, "Managing Groups."

### 10.12.6  Adding or Copying a Rule to a Policy

The **Copy Rule** button enables you to copy an existing rule to other policies.

## 10.13  Working with Trigger Combinations

Trigger combinations enable you to specify outcomes different from the ones for the individual rules. The outcomes are 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 nested policies to further evaluate the risk.

The trigger combinations evaluate sequentially, stopping as soon as a trigger combination is matched.

*Figure 10–8    Trigger Combination Structure*
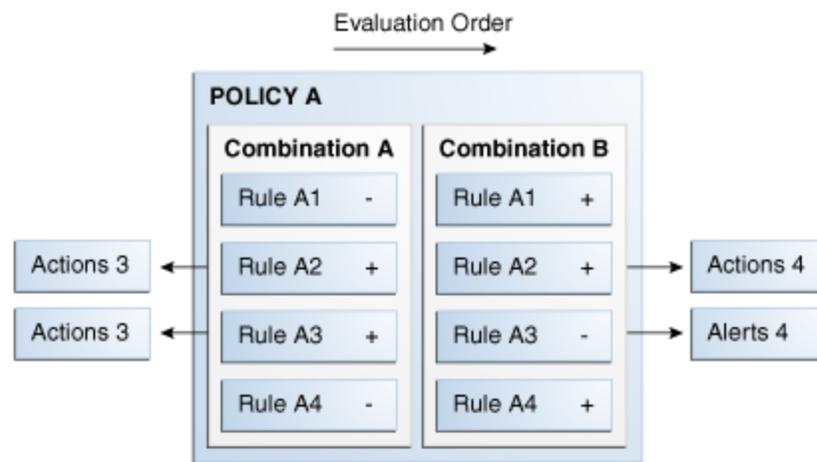
Trigger Combinations can be access through the **Rule Details** page. Each column in the table corresponds to a trigger combination.

*Figure 10–9   Trigger Combinations*
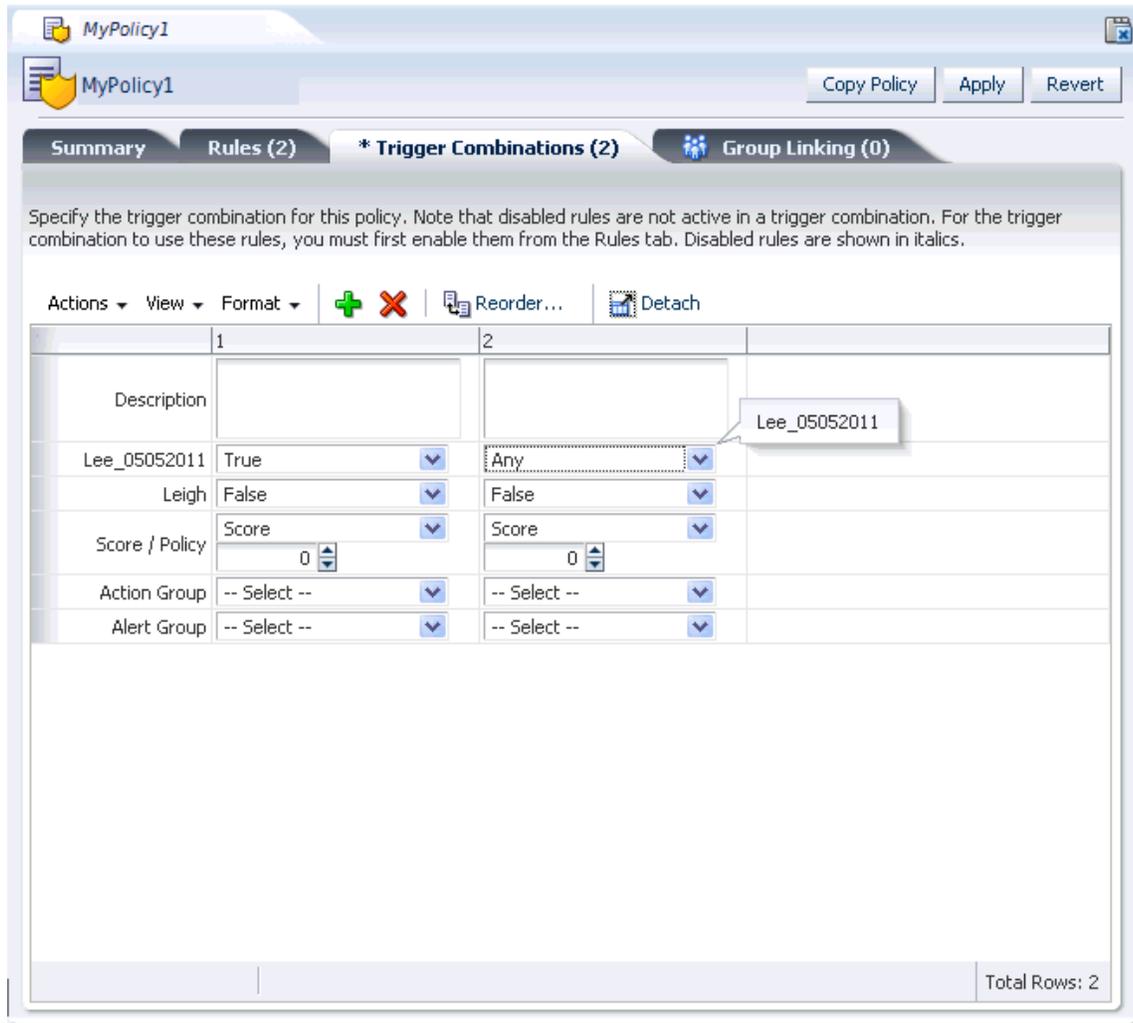


By default the rules are set to **Any**. **Any** ignores the rule whether or not it triggers.

The total number of trigger combinations in the policy appears in parenthesis next to the tab title.

The first column is frozen to enable you to scroll and see all of the data in the table while having the labels available for reference.

For information about Action and Alert groups, see Chapter 12, "Managing Groups."

*Table 10–5   Trigger Combination*

| Fields | Description |
|---|---|
| Description | Description for the trigger combination. Each trigger combination has a description. If the description is too long to display and part of it is obscured, you can place the mouse over the text to see the entire description. |
| Name | Name of the rule. |
| Score/Policy | If you select score, the score box appears where you can enter an integer value from 0 to 1000. The minimum and maximum scores for the Score are defined as properties.<br><br>Scores of 0 or less than 0 are ignored.<br><br>If you select Policy, a policy list appears with policies of same checkpoint. |

*Table 10–5   (Cont.)  Trigger Combination*

| Fields | Description |
| --- | --- |
| Policy | If you select policy, the nested policy must be configured to run in the same checkpoint. |
| Action Group | An action group indicates all the actions that must occur when the rule is triggered. |
| Alert Group | An alert group is made up of graded messages that are used as results within rules so that when a rule is triggered all of the alerts within the groups are activated. |

Table 10–6, " Trigger Combination Toolbar Options" lists the commands that are available through the toolbar.

There is no limit to the number of trigger combinations that you can add.

By default, if a policy does not have any trigger combination, a table is created with all the rules in the policy and one column for the trigger combination. You can make edits to the combination and then save it.

You can provide the description and other values to the trigger combination. By default, when the combination is added, **Apply** and **Revert** are enabled, even if you do not make edits to the new combination.

You can edit multiple trigger combinations and save them all at once.

If you navigate away from the tab while editing the trigger combination, the trigger combination is saved in the session and available when you navigate back.

Columns can be reordered using the **Reorder** button.

> **Note:**   Note that the **Add**, **Delete**, and other operations are irreversible. Ensure that you are ready to perform these operations before proceeding.

*Table 10–6   Trigger Combination Toolbar Options*

| Command | Description |
| --- | --- |
| Add | This button adds a new column (trigger combination). |
| Delete | This button is enabled only if a column or row is selected. The Delete button also enables you to delete multiple trigger combinations. When the **Delete** button is clicked, a warning message appears, asking for confirmation. |
| Reorder | This button invokes the Reorder screen. |

## 10.13.1  Specifying Trigger Combinations

To specify trigger combinations:

1.  In the Navigation tree, select **Policies**. The **Policies Search** page is displayed.

2.  Search for the policy which you want.

3.  Click the policy name to open its **Policy Details** page.

4. Navigate to the **Trigger Combinations** tab.

5. Select the return value permutations you want for each rule in the first column.

6. In the **Score/Policy** row, select **Score** or **Policy** to specify whether the result return a score or point to a nested policy.

   ■ If you selected **Score**, in the field directly below, specify the score you want to assign to that combination.

   ■ If you selected **Policy**, in the field directly below, specify the policy you want to run to further evaluate the risk.

   Only the list of policies of the same checkpoint are available.

7. Set an action outcome.

8. Set an alert outcome:

9. If you want to specify other trigger combinations, click **Add** to add another column.

10. Repeat Steps 5 through 8 for each trigger combination you want.

11. In the **Trigger Combinations** tab, click **Apply** after making all your edits.

You cannot add two trigger combinations of the same combination. When you add new combinations, each combination is saved and validated automatically.

If you navigate away from the tab while editing trigger combinations, the unsaved trigger combinations are saved in the session and available when you navigate back.

### 10.13.2 Changing the Sequence of the Trigger Combination

To change the order of trigger combinations:

1. In the Navigation tree, select **Policies**. The **Policies Search** page is displayed.

2. Search for the policy which you want.

3. Click the policy name to open its **Policy Details** page.

4. Navigate to the **Trigger Combinations** tab.

5. To reorder columns, click the **Reorder** button.

   The **Reorder Trigger Combinations** screen appears.
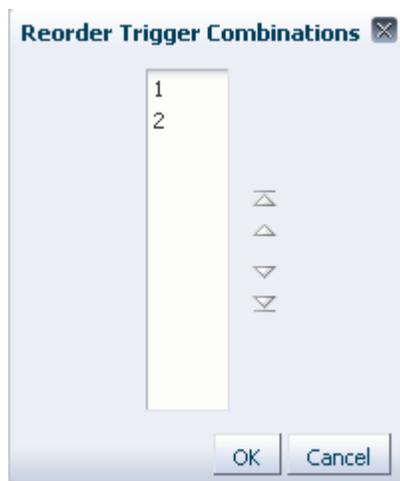
6. Reorder the trigger combinations and click **OK**.

7. In the **Trigger Combinations** tab, click **Apply**.

Reordering of trigger combinations takes effect only after you click **Apply**. The changes are lost if you close the tab before you click **Apply**.

### 10.13.3 Deleting a Trigger Combination

To delete a trigger combination:

1. In the Navigation tree, select **Policies**. The **Policies Search** page is displayed.

2. Search for the policy which you want.

3. Click the policy name to open its **Policy Details** page.

4. Navigate to the **Trigger Combinations** tab.

5. Select the column header corresponding to the trigger combination and click **Delete**.

## 10.14 Deleting Policies

To delete policies:

1. In the Navigation tree, select **Policies**. The **Policies Search** page is displayed.

2. In the **Policies Search** page, search for the policy or policies you want to delete.

   For information on searching for a policy, see Section 10.5, "Searching for a Policy."

3. Select the policies you want to delete and click the **Delete** button or select **Delete Selected** from the **Action** menu.

   A **Confirm Delete** dialog appears, asking for confirmation. If you selected to delete more than one policy, a list of policies is shown in the dialog.

4. Click **Delete**.

   An information screen appears.

5. In the information screen, click **OK**.

   The policy deleted successfully.

   You cannot undo the delete. The changes are permanent.

## 10.15 Copying a Rule to a Policy

You can copy a rule to a different policy under any checkpoint. For example, you want to move the rule to a different checkpoint.

*Figure 10–10   Overview of Copying a Rule*
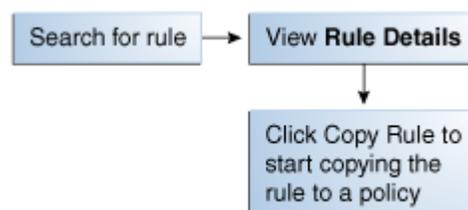
To copy a rule to a policy:

1. In the Navigation tree, select **Rules**. The **Rules Search** page is displayed.

2. Enter the search criteria you want and click **Search**.

3. In the **Search Results** table, click the name of the rule you want to copy to a policy.

   The **Rule Details** page for that rule is displayed.

4. In the **Rule Details** page, click the **Copy Rule** button.

   The **Copy Rule** page appears pre-populated with the rule name and description from the original rule.

5. In the **Policy** field, select the policy you want to copy the rule to.

6. In the **Rule Name** field, enter a new name for the rule that you are copying.

7. In the **Description** field, enter a description for the rule.

8. Click **Copy** to copy the rule to the policy.

## 10.16 Copying a Policy to Another Checkpoint

You can copy a policy to other checkpoints.

1. In the Navigation tree, select **Policies**. The **Policies Search** page is displayed.

2. Enter the search criteria you want and click **Search**.

3. Click the policy name to open its **Policy Details** page.

4. In the **Policy Details** page, click **Copy Policy**.

   You can access the **Copy Policy** button from any tab in the **Policy Details** page.

   The **Copy Policy** screen appears with all the fields pre-populated.

   Table 10–7, " Copy Policy to Checkpoint" lists the fields in the **Copy Policy** screen.

*Table 10–7    Copy Policy to Checkpoint*

| Field | Description |
| --- | --- |
| Checkpoint | The checkpoint you are copying the policy to. By default the field is pre-populated with the checkpoint from the policy that is being copied. |
| Policy Name | Default value for Policy Name field is *policy_name*Copy. You can edit the policy name, if needed. |
| Status | The policy status of "disabled" is set as the default value. Defines the state of the object or its availability for business processes. For information, refer to **Policy Status**. |
| Description | Current description is set as the default description. |

5. In the **Copy Policy** screen, select the checkpoint and status.

6. Enter a policy name and description.

7. In the **Copy Policy** screen, click **Copy**.

   If you click **Copy**, the policy is copied to the checkpoint.

If the rules of the policy are not applicable (cannot be copied) to the new checkpoint, a "The following rules are not applicable for this checkpoint" message appears.

You are given the option either to abort the copy operation or to continue copying the policy without those rules.

When policies are copied, all the details are copied including the nested policies, trigger combinations, preconditions, group linking, and so on.

## 10.17 Exporting and Importing a Policy

Policies can be exported and imported.

For example, you can export the policies defined in a system and import them into another system.

### 10.17.1 Exporting a Policy

To export policies:

1. In the Navigation tree, select **Policies**. The **Policies Search** page is displayed.

2. Enter the search criteria you want and click **Search**.

3. Select the rows corresponding to the policies you want to export.

4. From the **Actions** menu, select **Export selected** or **Export Delete Script**.

5. When the export screen appears, select **Save File**, and then **OK**.

### 10.17.2 Importing a Policy

**Note for Policies Migrated from 10*g* to 11*g***

Only security policies are available in 11*g*. Business, third-party, workflow policy types have been removed from Oracle Adaptive Access Manager.

In 10*g*, scoring was not used by business policies. In 11*g*, when business policies are loaded from the Oracle Adaptive Access Manager database, the policy set scoring engine is applied by default and these policies are treated as security policies from 11*g* onward.

To import policies:

1. Create a \tmp folder in the drive where you have installed WebLogic if OAAM Admin is installed on the Windows platform.

   For example, if the WebLogic domain is on the C drive, you would create a c:\tmp folder.

   This folder is used as a temporary folder for uploading large files into the OAAM Admin application.

2. In the Navigation tree, select **Policies**. The **Policies Search** page is displayed.

3. In the **Policies Search** page, click the **Import Policy** button. The **Import Policy** screen appears.

*Figure 10–11   Import Policy*
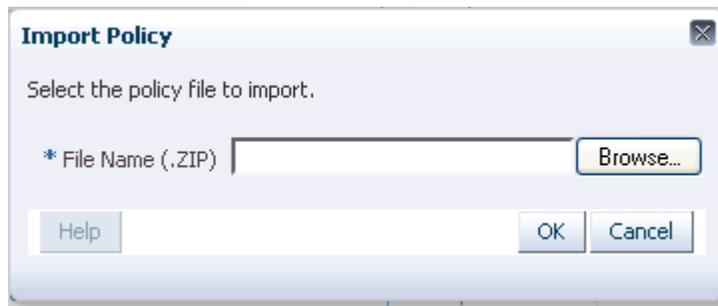


4. In the **Import Policy** dialog box, type the path and name of the file; or use the **Browse** (...) button to locate the ZIP file that contains the policies, and then select the file.

   Note: a validation is performed for the imported file's MIME type. The MIME type of the export file should be "Application/ZIP."

5. Click **Open** and then click **OK**.

   A confirmation dialog appears with the list of policies and the number of policies that were added, updated, not updated, or not deleted in the system after the import.

   The policies are imported into the system unless the ZIP file contains a delete script or files in an invalid format or the ZIP file is empty.

   If you are importing a delete script, the policies are deleted from the system.

   An error occurs if you try to import policies in an invalid format or an empty ZIP file.

6. Click **Done** to dismiss the confirmation dialog.

## 10.18 Navigating to the Rules Search Page

To open the **Rules Search** page, right-click the **Rules** node in the Navigation tree. The **Rules Search** page is displayed.

Alternatively, you can open the **Rules Search** page by:

- Right-clicking **Rules** in the Navigation tree and selecting **List Rules** from the context menu.

- Selecting **Rules** in the Navigation tree and then choosing **List Rules** from the **Actions** menu.

- Clicking the **List Rules** button in the Navigation tree toolbar.

An example of a **Rules Search** page is shown in Figure 10–12, "Rules Search Page".

*Figure 10–12   Rules Search Page*



## 10.19  Searching for Rules

The **Rules Search** page displays a Search filter and a **Search Results** table that shows a summary of the rules that match your search criteria.

From the **Rules Search** page, you can view and edit the details of the rule, but you cannot create a rule. Rules can only be created in the context of policies.

1. In the Navigation tree, select **Rules**. The **Rules Search** page is displayed.

2. In the **Rules Search** page, enter the search criteria you want.

3. Click **Search**.

   Clicking **Reset** instead of **Search** resets the search criteria.

The **Search Results** table displays a summary of rules that meet the criteria you specified.

*Table 10–8    Rules Results*

| Field | Description |
|---|---|
| Rule Name | Name of the rule |
| Policy Name | Name of the policy where the rule resides. |
| Checkpoint | Point during the session the rules in a policy are evaluated. |
| Rule Notes | Description for the rule. |
| Rule Status | Status of the rule: Active or Disabled. If the rule status is changed from Active to Disabled, the rule is disabled and cannot be added to a policy. A policy that already contains the rule is not affected and continues to function as before. |
| Action Group | Group of actions. An action group indicates all the actions that must occur when the rule is triggered. By default, actions are not specified. You must specify a set of results for the rule. |
| Score | Integer value from 0 to 1000. The minimum and maximum scores for the Score are defined as properties. |
| Weight | Integer value from 0 to 100 |

The **Delete** button or **Delete Selected** from the **Action** Menu enables you to delete rules. The **Delete** and **Delete Selected** are enabled only if a row is selected.

The delete operation either succeeds or fails. There are no partial updates made.

The option to sort is provided on every column in the **Search Results** table.

Each rule has a name. If the description is too long to be fully shown, you can place the mouse over the text to see the entire description.

To view and edit the rule details, click the rule name in the **Search Results** to open the rule.

## 10.20  Viewing Rule Details

To view the details of a rule:

1.  In the Navigation tree, select **Rules**. The **Rules Search** page is displayed.

2.  Search for the rule in which you want to view the details.

3.  Click the rule name in the **Search Results** table or select the row and select **Open Selected** from the **Action** menu to open its **Rule Details** page in a new tab.

The **Rule Details** page enables you to access the complete details of a rule through four tabs. These pages allow the management of the rule.

The **Rule Details** page has four tabs

- General

- Preconditions

- Conditions

- Results

These tabs allow the management of the rule.

Figure 10–13 illustrates the tabs in the Rule Details page and the information to enter for each tab.

*Figure 10–13  Policies*
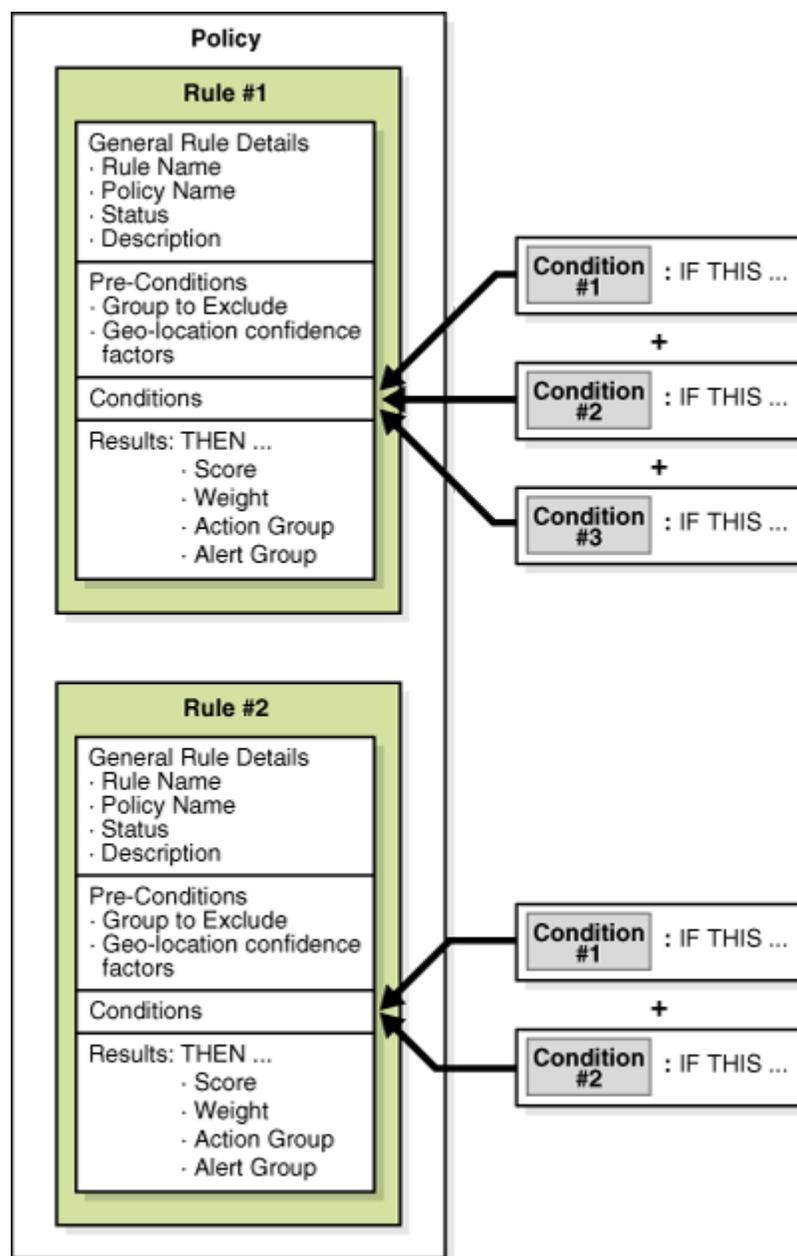


## 10.21  Editing Rules

To edit a rule:

1. In the Navigation tree, select **Rules**. The **Rules Search** page is displayed.

2. Search for the rule which you want to edit.

3. Click the rule name in the **Search Results** table to open its **Rule Details** page in a new tab.

   The **Rule Details** page provides tabs to the **Summary**, **Preconditions**, **Conditions**, and **Results** page.

The total number of conditions in the rule appears in parenthesis next to the Conditions tab title.

4. Edit the rule's general information (Section 10.21.1, "Modifying the Rule's General Information").

5. Edit the Preconditions (Section 10.21.2, "Specifying Preconditions").

6. Edit/Add Conditions (Section 10.27, "Adding Conditions to a Rule").

7. Edit the Results (Section 10.21.3, "Specifying the Results for a Rule").

8. Click **Apply** to save the changes or **Revert** to discard them.

### 10.21.1 Modifying the Rule's General Information

From the **Summary** tab, you can modify the rule name, status, and description.

*Figure 10–14 Rule Details Summary Tab*



The fields displayed are listed in Table 10–9.

*Table 10–9    Rule Details Summary Tab*

| Field | Description |
| --- | --- |
| Rule Name | Name of the rule |
| Policy Name | Name of the policy. (Read-only) |
| Status | Status of the rule: Active or Disabled. If the rule status is changed from Active to Disabled, the rule is disabled and cannot be added to a policy. A policy that already contains the rule is not affected and continues to function as before. |
| Description | Description for the policy. |

## 10.21.2 Specifying Preconditions

From the **Preconditions** tab, you can specify the group to exclude and the geolocation confidence factor parameters.

All preconditions filter whether or not a rule evaluates. The conditions do not process the rule if the preconditions are not met. The process stops at the preconditions level.

To specify preconditions for the rule:

1.  Navigate to the **Rule Details** page.

    a.  In the Navigation tree, select **Rules**. The **Rules Search** page is displayed.

    b.  Search for the rule in which you want to specify preconditions for.

    c.  In the **Search Results** table, click the name of the rule. The **Rule Details** page for that rule is displayed.

2.  In the **Rule Details** page, click the **Preconditions** tab.

3.  **Excluded User Group**: In the **Excluded User Group** field, select the User ID group you do not want the policy to applied to.

4.  **Device Risk Gradient**: Device fingerprinting is a mechanism to recognize the device a customer typically uses to log in. Identification is based on combinations of the Device ID attributes, secure cookie, flash object, user agent string, browser characteristics, device hardware configuration, network characteristics, geolocation and historical context.

    Different use cases and exceptions are taken into account and help to define the device risk gradient. The device risk gradient specifies the certainty of the device being identified. It is standard in almost all rules as a precondition.

    The score ranges to specify the amount of device identification risk are:

    ■  400 and lower - low risk

    ■  401-700 -  moderate risk

    ■  701 and higher -  high risk

    For example, a device risk gradient of 0 is an exact match whereas a device gradient of 500 is a "similar" device, and a score of 1000 a "different" device.

5.  **Country Confidence Factor**, **State Confidence Factor**, and **City Confidence Factor**: The IP location vendor can assign a confidence level to each of the three elements: city, state, and country. This confidence factor is based on IP geolocation information.

    The higher the value, the higher the level of confidence from Quova that the mapping of the location is correct.

If you want the rule you are creating to be dependent on IP location identification accuracy, specify the amount of geolocation accuracy with which you want to run the rule.

For example, if the range is 60 to 100, you may specify for the rule to run only if the IP location is greater than 60% positive.

### 10.21.3 Specifying the Results for a Rule

Results are the responses, such as the activation of an action and message, when a rule is triggered. For example, action (event activated) and alert (message activated).

As part of the process, specify:

- Rule score and weight value

- Actions

- Alerts

To specify the results for if the rule triggers, follow these steps:

1. Navigate to the **Rule Details** page if you are not on the **Rule Details** page of the rule you want.

   a. In the Navigation tree, select **Rules**. The **Rules Search** page is displayed.

   b. Search for the rule for which you want to specify the results.

   c. In the **Search Results** table, click the name of the rule. The **Rule Details** page for that rule is displayed.

2. In the **Rule Details** page, click the **Results** tab.

3. Enter a rule score and weight value.

   You can change the weight value for a rule to instruct OAAM Admin to give more or less value to the total score.

   By default the score is 1000 and the weight is 100.

4. In the **Actions Group** list, select the actions you want triggered by this rule, if actions are required.

   By default, an **Actions Group** is not selected.

5. In the **Alerts Group** list, select the alerts you want sent if this rule is triggered.

   By default, an **Alerts Group** is not selected.

6. Click **Apply** to save the modified rule details.

The rules engine takes the information you specify for the rule and information specified in other rules in the policy and returns rule results to the policy. All the policies in the policy set results in multiple actions and multiple scores and multiple alerts. All these are propagated to the checkpoint. The score, the weight, and so on result in one final score, one final action, and a couple of alerts.

An example of a final action is **Block**. An example action list is **Block**, **Challenge**, **Background Check** and an example score is 800.

*Table 10–10    Results Tab*

| Field | Description |
| --- | --- |
| Score | Integer value from 0 to 1000. The minimum and maximum scores for the Score are defined as properties. |
| Weight | Integer value from 0 to 100 |
| Action Group | Group of actions. An action group indicates all the actions that must occur when the rule is triggered. |
| Alert Group | Group of graded messages that are used as results within rules so that when a rule is triggered all of the alerts within the groups are activated. |

## 10.22 Working with Scores and Weights

For information about the processing of policies to come up with scores, actions, and alerts, see Chapter 14, "Using the Scoring Engine."

## 10.23 Activate/Disable Rule

To activate/disable a rule:

1. In the Summary tab of Rule Details, select **Active** or **Disable** for **Status**.

   If the rule status is changed from **Active** to **Disabled**, the rule is disabled and cannot be added to a policy. A policy that already contains the rule is not affected and continues to function as before.

2. Click **Apply**.

## 10.24 Deleting Rules

To delete rules:

1. In the Navigation tree, select **Rules**. The **Rules Search** page is displayed.

2. Search for the rule you want to delete.

3. Select the rows corresponding to the rules of interest and press the **Delete** button or select **Delete Selected** from the **Actions** menu.

   A **Confirm Delete** dialog appears withe a list of rules to be deleted.

   The delete operation either succeeds or fails. There are no partial updates made.

4. Click the **Delete** button.

   If you delete the rule, the corresponding row are deleted in the trigger combinations where this rule was used.

5. When the confirmation appears, click **OK**.

## 10.25 Searching Conditions

The Conditions Search page displays a Search filter and a Search Results table that shows a summary of the conditions that match your search criteria.

For a list of conditions, see Appendix C, "Conditions Reference."

From the Conditions Search page, you can search for a condition or a list of conditions in the system.

1. From the Navigation tree, click **Conditions**.

   The **Conditions Search** page is displayed.

   Alternatively, you can open the **Conditions Search** page by:

   - Right-clicking **Conditions** in the Navigation tree and selecting **List Conditions** from the context menu.

   - Selecting **Conditions** in the Navigation tree and then choosing **List Conditions** from the **Actions** menu.

   - Clicking the **List Conditions** button in the Navigation tree toolbar.

2. Enter the search criteria you want and click **Search**.

   Clicking **Reset** instead of **Search** resets the search criteria.

   Table 10–11, " Conditions Search fields" lists the fields in the Search section.

*Table 10–11    Conditions Search fields*

| Field | Description |
|---|---|
| Condition Name | Name given to the condition. |
| Description | Description of the condition |
| Type | Type of condition. For example, Device, Location, and User. |
| Checkpoints | Point during the session the rules in a policy are evaluated. |

Each condition has a name. If the description is too long to be fully shown, you can place the mouse over the text to see the entire description.

Click the name of the condition you are interested in to view more details.

## 10.26 Importing Conditions

To import a condition:

1. From the Navigation tree, click **Conditions**.

   The **Conditions Search** page is displayed.

2. Click **Import Conditions**.

3. In the **Import Conditions** dialog box, type the path and name of the file; or use the **Browse** (...) button to locate the ZIP file that contains the conditions, and then select the file.

4. Click **Open** and then click **OK**.

   A confirmation dialog appears with the list of conditions and the number of conditions that were added, updated, not updated, or not deleted in the system after the import.

5. Click **Done** to dismiss the confirmation dialog.

## 10.27 Adding Conditions to a Rule

The **Rule page**'s **Condition** tab displays the conditions in the rule and enables you to add other conditions and customize them.

*Figure 10–15  Adding conditions*



Follow these steps to add a condition:

1.  If you are not on the **Rule Details** page of the rule in which you want to add the condition to, navigate to that page.

    a.  In the Navigation tree, select **Rules**. The **Rules Search** page is displayed.

    b.  Search for the rule in which you want to add the condition for.

    c.  In the **Search Results** table, click the name of the rule. The **Rule Details** page for that rule is displayed.

2.  In the **Rule Details** page, click the **Conditions** tab.

3.  In the **Conditions** tab, click **Add**. The **Add Condition** page appears.

4.  Search for the condition you want for the rule.

5.  In the **Search Results** table, select that condition and click **Add**.

*Figure 10–16   Add Conditions*
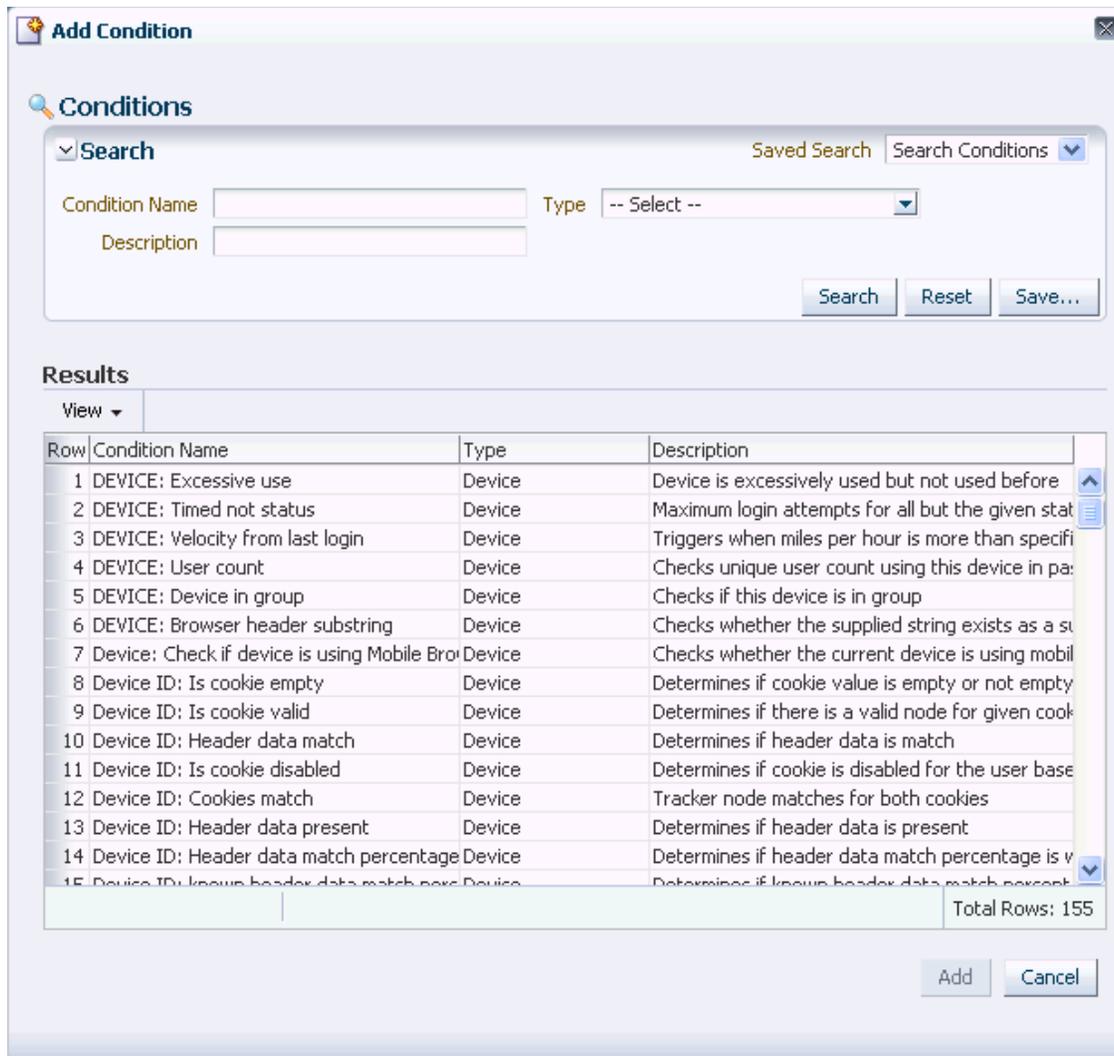


6.  In the **Conditions** edit page, select the condition in the top subtab.

    The bottom subtab displays the parameters of the condition.

7.  In the bottom subtab, modify the parameters per your requirements.

8.  Click **Save** to save your changes.

    A confirmation dialog displays the status of the operation.

9.  Click **OK** to dismiss the confirmation dialog.

10. Click **Apply**. The modified rule details were saved successfully.

    An example of the **Conditions** tab is shown in Figure 10–17, "Condition Parameters".

*Figure 10–17   Condition Parameters*
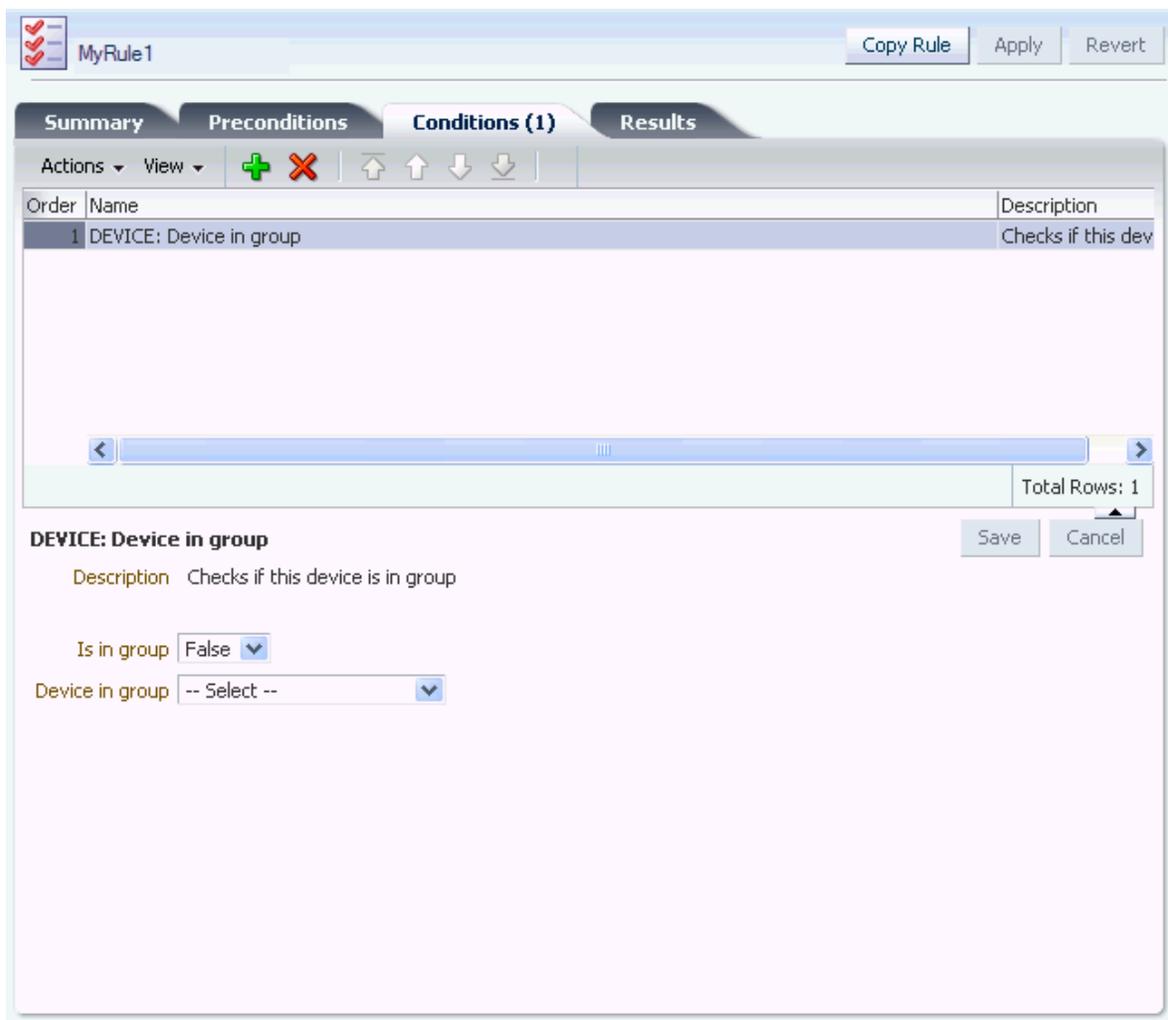


The top tab displays the conditions in the rule.

Table 10–12 lists the fields in the top subtab of the **Conditions** tab.

*Table 10–12   Rule Details Conditions Tab*

| Fields | Descriptions |
| --- | --- |
| Order | Order of the condition. Conditions in the rule 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 must 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. |
| Condition Name | Name of the condition. |
| Description | Description of the condition. |

You can only view/edit one condition's parameters at a time.

## 10.28 Viewing the Condition Details of a Rule

To view the details of a condition:

1. Navigate to the **Rule Details** page of the rule.

    a. In the Navigation tree, select **Rules**. The **Rules Search** page is displayed.

    b. Search for the rule in which you want to add the condition for.

    c. In the **Search Results** table, click the name of the rule. The **Rule Details** page for that rule is displayed.

2. In the **Rule Details** page, click the **Conditions** tab.

3. In the **Conditions** tab, highlight the condition you are interested in.

    The bottom subtab displays the parameters for the condition.

## 10.29 Exporting a Condition

1. In the Navigation tree, select **Conditions**. The **Conditions** page is displayed.

2. Enter the search criteria you want and click **Search**.

3. Select the rows corresponding to the conditions of interest.

4. From the **Actions** menu, select **Export selected**.

5. When the export dialog appears, select **Save File**, and then **OK**.

## 10.30 Editing Conditions

The **Conditions** tab of the **Rule Details** page displays the conditions in the rule and enables you to customize conditions within the rule.

To edit a condition in a rule:

1. In the Navigation tree, select **Rules**. The **Rules Search** page is displayed.

2. Search for the rule which you want to edit.

3. Click the rule name in the **Search Results** table to open its **Rule Details** page in a new tab.

    The **Rule Details** page provides the **Summary**, **Preconditions**, **Conditions**, and **Results** tabs.

4. In the **Rule Details** page, click the **Conditions** tab.

5. In the **Conditions** tab, select the condition in the top subtab.

    The bottom subtab displays the parameters of the condition.

6. Use the **Reorder** buttons on the tool menu to change the order of the conditions.

    See Section 10.31, "Changing the Order of Conditions in a Rule" for details.

7. In the bottom subtab, modify the parameters per your requirements.

8. Click **Save** to save your changes.

    A confirmation dialog displays the status of the operation.

9. Click **OK** to dismiss the confirmation dialog.

10. Click **Apply**. The modified rule details were saved successfully.

## 10.31 Changing the Order of Conditions in a Rule

Conditions in the rule 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.

To change the order of a condition in a rule:

1. In the Navigation tree, select **Rules**. The **Rules Search** page is displayed.

2. Search for the rule which you want to edit.

3. Click the rule name in the **Search Results** table to open its **Rule Details** page in a new tab.

   The **Rule Details** page provides the **Summary**, **Preconditions**, **Conditions**, and **Results** tabs.

4. In the **Rule Details** page, click the **Conditions** tab.

5. In the **Conditions** tab, select the condition in the top subtab.

6. Use the **Reorder** buttons reorder the condition.

7. Click **Save** to save your changes.

   A confirmation dialog displays the status of the operation.

8. Click **OK** to dismiss the confirmation dialog.

9. Click **Apply**. The modified rule details were saved successfully.

## 10.32 Deleting Conditions

To delete conditions:

1. In the Navigation tree, select **Conditions**. The **Conditions Search** page is displayed.

2. Enter the search criteria for the conditions you are interested in and click **Search**.

3. Select the conditions in the **Search Results** table and click **Delete**.

   > **Note:** If rules are using the condition, deleting it affects the rules and policies that use it.

## 10.33 Deleting Conditions from a Rule

To delete a condition from a rule:

1. In the Navigation tree, select **Rules**. The **Rules Search** page is displayed.

2. Search for the rule that contains the conditions you want to delete.

3. Click the rule name in the **Search Results** table to open its **Rule Details** page.

4. In the **Rule Details** page, click the **Conditions** tab.

5. Select the condition of interest and click **Delete**.

   The **Delete** button is enabled only if a row is selected or the search result has at least two rows.

   You cannot delete multiple conditions at a time in a given rule; you must select one condition at a time.

You can delete more than one condition, but not all conditions can be deleted.

When the **Delete** button is clicked, the deletion is performed. You do not receive a message asking if you are sure you want to delete. The change is permanent.

## 10.34 Use Cases

This section describes example use cases for policies and rules.

### 10.34.1 Use Case: Rule Exception Group

Jeff, a Security Administrator, must create an exception user group to be used as a rule precondition. Jeff is creating a blacklisted country rule and realizes he should have an exception group so he creates a new user group named "BLC: exception users." In the description he enters a note that CSR managers can add users that need to be permanently allowed access from a blacklisted country. When created, the user group is added as the precondition. After the rule is in production a CSR manager assists a user who has moved to a blacklisted country. He manually adds his User ID to the group so he has an exception to the rule and adds a note in his case to this effect.

1. Create a new user group named "BLC: exception users."

   Group name: **BLC: exception users**

   Group type: **User ID**

   In the description, enter a note to tell investigators, **Add users that need to be permanently allowed access from a blacklisted country**.

2. Select existing User IDs to add to the **BLC: exception users** group.

   For information on creating user groups and then adding members, refer to Section 12.13, "Searching for and Adding Existing Elements or Creating and Adding a New Element."

3. Create a rule in a post-authentication blacklisted country policy.

   ■ For rule condition, choose **Location: IP in group**.

   ■ In **Pre-condition**, select **BLC: exception users** as the exception group.

4. After the rule is in production an investigator assists a user who has moved to a blacklisted country. He manually adds his User ID to the group so he has an exception to that rule and adds a note in his case to this effect.

### 10.34.2 Use Case: Import Policy

You are Jennifer, a member of the security team at Acme Corp. You must configure Oracle Adaptive Access Manager to accomplish one of the use cases the team came up with focusing on high risk countries. Chuck, another team member, configured a pre-authentication policy in the Oracle Adaptive Access Manager offline environment to block login requests from high risk countries before authentication. You know this policy can work for your purposes. Chuck already exported the policy and now you must import it into production. Directions: Import the ZIP file that contains Chuck's configured policies. He has name the file, PreAuth_Block_policy.zip.

To import a policy:

1. Log in to OAAM Admin as an administrator.

2. In the Navigation tree, select **Policies**. The **Policies Search** page is displayed.

3. Click **Import Policy** in the **Policies Search** page. The **Import Policy** screen is displayed.

4. Click **Browse** and search for `PreAuth_Block_policy.zip`.

5. Click **OK** to upload `PreAuth_Block_policy.zip`.

   A confirmation dialog displays the status of the operation.

   A list also appears showing numbers for **Number of Policies Added**, **Number of Policies Updated**, **Number of Policies Not Updated**, and **Number of Policies Deleted**.

   The imported policy is listed in the **Imported List** section.

   The policy is added to the system or it overwrites/updates an existing policy depending on whether the same policy name exists. If the name already exists, the policy is updated. If the name does not exist, the imported policy is added to the system.

   An error is displayed if you try to import files in an invalid format or an empty ZIP file.

6. Click **OK** to dismiss the confirmation dialog.

7. In the **Policy Search** page, verify that the policy appears in the **Search Results** table.

## 10.34.3 Use Case: Create a Policy

You must configure a login use case that can result in a KBA challenge. It is usually best practice to use KBA challenges only after successful authentication by the primary method. A post-authentication KBA challenge policy did not already exist so you must create a new one. The security team wants this policy to be applied to all users in the deployment. Directions: Create a new post-authentication KBA challenge policy that applies to all users. Name the policy, **KBA Challenge**.

To create a policy:

1. Log in to OAAM Admin as an administrator.

2. In the Navigation tree, double-click **Policies**.

3. In the **Policies Search** page, click the **New Policy** button.

   The **New Policy** page appears. In the **Summary** tab, the default values for the new policy are displayed as follows:

   - Policy Status: **Active**

   - Checkpoint: **Pre-Authentication**

   - Scoring Engine: **Average**

   - Weight: **100**

4. Create a new post-authentication security policy.

   a. For Policy Name, enter **KBA Challenge**.

   b. For **Description**, enter a description for the KBA Challenge policy.

   c. For **Checkpoint**, select **Post-Authentication**.

      For information on checkpoints, see Section 10.1.4, "Checkpoints."

    **d.** Modify the policy status, scoring engine, and weight according to your requirements.

    By default, the policy status is **Active**. A policy that is disabled is not enforced at the checkpoint.

    For more information on the Scoring Engine, see Chapter 14, "Using the Scoring Engine."

    **e.** Click **Apply**.

    A confirmation dialog displays the status of the operation.

    If you click **Apply** and the required fields are not filled in an error message is displayed.

    **f.** Click **OK** to dismiss the confirmation dialog.

**5.** Configure the policy to run for all users.

    **a.** Click the **Group Linking** tab.

    **b.** For **Run Mode**, select **All Users**.

    Since **All Users** is selected for the run mode, the policy is executed (run) for all users.

    Specifying a run mode is a mandatory step in order for the policy to execute. It enables the policy to execute/run for a set of users or all users. For information, see Section 10.9, "Linking Policy to All Users or a User ID Group."

    **c.** Click **Apply**.

    A confirmation dialog displays the status of the operation.

    **d.** Click **OK** to dismiss the confirmation dialog.

If the KBA Challenge policy was created successfully, it would be listed in the **Search Results** table of the **Policies Search** page.

Although not covered in this use case, for the policy to function, you must add a rule to the policy either by creating a new rule within a policy (Section 10.12, "Adding a New Rule") or by copying an existing one (Section 10.15, "Copying a Rule to a Policy") to the policy.

### 10.34.4 Use Case: Add New Rule

After you have created a security policy (see Section 10.34.3, "Use Case: Create a Policy.") you are ready to create a new rule to perform the risk evaluation in your use case. The use case requires an evaluation of the physical distance between the location a user is logging in from now verses the last location he came from. This rule calculates the velocity/speed required to travel between the location given the time. The security team has determined that if the user appears to travel faster then 500 miles per hour between location and the device used is different then the user should be given a KBA challenge. Directions: Create a new rule, **User Velocity** and use the out-of-the-box condition, **User: Velocity from last successful login**.

To add a new rule:

**1.** Log in to OAAM Admin as an administrator.

**2.** In the Navigation tree, double-click **Policies**. The **Policies Search** page is displayed.

**3.** Search for KBA Challenge.

4.  In the **Search Results** table, click **KBA Challenge**. The **Policy Details** page for KBA Challenge is displayed.

5.  In the **Policy Details** page, click the **Rules** tab.

6.  In the **Rules** tab, click **Add** to add a new rule.
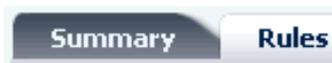


The New Rule page is displayed.

7.  Enter **User Velocity** as the rule name.

8.  Enter a description for the rule.

9.  Select the rule status.

    When the **New Rule** page first appears, the default value for the rule status is **Active**.

10. Add the **User: Velocity from last successful login** rule condition to create the new rule.

    a.  To add the **User: Velocity from last successful login** condition, click the **Conditions** tab.

    b.  In the **Conditions** tab, click **Add**. The **Add Condition** page appears.

    c.  Search for the **User: Velocity from last successful login** condition by entering **velocity** in the **Condition Name** field and then clicking **Search**.

    d.  In the **Results** table, select that condition and click **OK**.

    e.  In the **New Rule/User Velocity** page, select **User: Velocity from last successful login** in the top panel.

        The bottom panel displays the parameters of the condition.

    f.  In the bottom panel, modify the parameters.

        a.  Enter **500** for **Miles per Hour is more than**.

        b.  Select **true** for **Ignore if last login device is same**.

    g.  Click **Save** to save your changes. A confirmation dialog appears with a message that the modified rule parameters were saved successfully.

    h.  Click **OK** to dismiss the confirmation dialog.

11. Add a KBA challenge as a result of the **User Velocity** rule.

    a.  Click the **Results** tab.

        The **Results** tab enables you to specify the results for the rule if the conditions are met.

    b.  To set up a KBA challenge to occur if the rule is triggered, select **ChallengeQuestionPad** in the **Actions Group** list.

12. Click **Apply**. A confirmation dialog appears with a message that the modified rule details were saved successfully.

    If the required fields are not filled in and the user clicks **Apply**, an error is displayed.

    If the rule was successfully created, the new rule should be listed in the **Rules** tab of the **Policy Details** page.

**13.** Click **OK** to dismiss the confirmation dialog.

## 10.34.5 Use Case: Link Group to Rule Condition

In this use case, you must link an existing high risk countries group used for various purposes to a rule in the policy, **System - Pre Blocking**, you imported in

Directions: Find a high risk countries group and link it to the rule in the **KBA Challenge** policy, you created.

To link a group to a rule condition:

**1.** Log in to OAAM Admin as an administrator.

**2.** In the Navigation tree, double-click **Rules**. The **Rules Search** page is displayed.

**3.** Search for the **Blacklisted countries** rule.

**4.** In the **Search Results** table, click **Blacklisted countries**. The **Rule Details** page for the **Blacklisted countries** rule is displayed.

**5.** Select the **in group** rule condition in the **Blacklisted countries** rule.

    **a.** In the **Rule Details** page, click the **Conditions** tab.

    **b.** In the **Conditions** tab, click **Add**. The **Add Conditions** page appears.

    **c.** Search for the condition, **Location: In Country group**.

        The condition checks to see if the IP is in the given country group.

    **d.** In the **Search Results** table, select the **Location: In Country group** condition and click **OK**.

**6.** Link the existing high risk countries group to the rule condition.

    **a.** In the **Conditions** edit page, select the **Location: In Country group** condition in the top panel.

        The bottom panel displays the parameters of the condition.

    **b.** In the bottom panel, modify the parameters by setting:

        Is in list: **true**

        Country in country group: **Restricted countries**.

**7.** Click **Save** to save your changes. A confirmation dialog appears with a message that the modified rule parameters were saved successfully.

**8.** Click **OK** to dismiss the confirmation dialog.

**9.** Click **Apply**. A confirmation dialog appears with a message that the modified rule details were saved successfully.

## 10.34.6 Use Case: Copy Rule

The security team has determined that devices found to be exceptionally high risk should be blocked. Right now there is a rule to accomplish this but it was configured in a post-authentication checkpoint. The team feels login attempts should not even be allowed from these devices. Therefore you must move the rule to a pre-authentication checkpoint policy. Directions: Find the **Black-Listed Devices** rule in the **System -Post Blocking** policy and copy it to the pre-authentication policy, **System - Pre Blocking** policy. Then delete the rule from the post-authentication policy.

To copy a rule:

1.  Log in to OAAM Admin as an administrator.

2.  In the Navigation tree, double-click **Rules**. The **Rules Search** page is displayed.

3.  In Search filter, search for:

    ■   Rule Name: **Blacklisted device rule**

    ■   Checkpoint: **Post-Authentication**

4.  Click **Search**.

    The **System -Post Blocking** policy contains the **Blacklisted devices** rule.

5.  In the **Search Results** table, click **Blacklisted devices** in the **Rule Name** column.

6.  In the **Rules Details** page for that rule, click the **Copy Rule** button. The **Copy Rule** screen is displayed.

7.  For Policy, select **System - Pre Blocking** as the pre-authentication policy you want to copy the rule to.

8.  For **Rule Name**, keep **Blacklisted devices** or enter a new name for the rule that you are copying.

9.  For **Description**, keep **This rule triggers if the device used has been blacklisted in the past** or enter a new description.

10. Click **OK** to copy the rule to the pre-authentication policy, **System - Pre Blocking**.

    A confirmation dialog appears with the message, "Rule has been copied successfully."

11. Click **OK** to dismiss the dialog.

12. Navigate to the **Rules Search** page and check in the **Search Results** table to verify that the Blacklisted device rule appears in the **System - Pre Blocking** policy.

13. Navigate to the **Policies Search** page and search for the **System -Post Blocking** policy.

14. Click **System -Post Blocking** in the **Search Results** table.

15. In the **Policy Details** page, click the **Rules** tab.

16. In the **Rules** tab, select **Blacklisted devices** and click **Delete**.

    A screen appears asking, "Are you sure you want to delete the selected rules?" The **Blacklisted devices** rule is listed in the screen.

17. Click **Yes**.

    Another confirmation appears with the message, "Selected rules are deleted successfully."

18. Click **OK** to dismiss the dialog.

### 10.34.7  Use Case: Trigger Combination

To KBA challenge a user Oracle Adaptive Access Manager must check two things:

■   First, check to see whether the user has challenge questions registered.

■   Second, if the user has a questions set active challenge him if a challenge scenario has to be performed.

To configure this behavior you must nest your new security policy, which contains rules that can result in a KBA challenge, under the policy, which contains KBA business rules to check for registration status.

Directions: Nest the **KBA Challenge** policy under the **System - Questions check** policy using policy trigger combinations.

The **KBA Challenge** policy was created in

To create a trigger combination:

1. Log in to OAAM Admin as an administrator.

2. In the Navigation tree, double-click **Policies**. The **Policies Search** page is displayed.

3. Search for the **System - Questions** check policy.

4. In the **Search Results** table, click **System - Questions check**. The **Policy Details** page for the **System - Questions check** policy is displayed.

5. In the **Policy Details** page, click the **Trigger Combinations** tab.

6. In the **Trigger Combinations** tab, click **Add**.

   The column added to the table corresponds to a trigger combination.

   By default, trigger combinations are created with all the rules in the policy. The rules used in the policy are represented by a row name.

   For example, the rules to check for registration status would appear as rows:

   - Registered User with condition **User: Account Status**

   - Question Registered

   - Unregistered User

7. In the trigger combination, enter a description in the **Description** field.

8. For each rule specify the rule result based on which trigger combination must be executed (performed)

   - **True**: The rule is triggered

   - **False**: the rule is not triggered

   - **Any**: Ignore the rule whether or not it triggers

   By default, a trigger combination is executed for a rule result of **Any**.

9. For a trigger combination, specify that if the trigger combination triggers, the result returns a nested policy.

   Select **Policy**, and in the field directly below, specify **KBA Challenge** as the policy you want to run to further evaluate the risk.

   A nested policy is a secondary policy used to further quantify the risk score in instances where the original result output by the system is inconclusive. Nested policies can be assigned to ensure a higher degree of accuracy for the risk score.

10. Select the **Action Group**.

    The action is an event generated when the combination is triggered.

11. Select the **Alert Group**.

    The alert is a message generated when the combination is triggered.

**12.** Click **Apply**. A confirmation dialog is displayed, saying that the policy details were updated successfully.

**13.** Click **OK** to dismiss the dialog.

## 10.34.8  Use Case: Trigger Combination and Rule Evaluation

Jeff, a Security Administrator, must configure two levels of authentication to challenge the user using KBA for any single rule trigger and OTP for specific combinations of rules triggering.

The tasks he must perform are the following:

- Create a pattern to profile user login times into 4 hour time range buckets.

- Create a second pattern to profile states users log in from.

- Create the rules to use these patterns in the KBA challenge policy so these evaluations only run if the user has KBA active.

- Create a rule to challenge using KBA if the user falls into a login time bucket he has fallen into less than 10% of the time in the last month.

- Next, create a rule to challenge using KBA if the user logs in from a state he has used less than 20% of the time in the last two weeks.

- Then, create a rule that checks to see if a user has an OTP delivery channel active.

- Finally, configures a trigger combination to OTP challenge the user if all three of these rules returns true.

The steps to accomplish these tasks are:

**1.** Log in to OAAM Admin as an administrator.

**2.** In the Navigation tree, select **Patterns**. The **Patterns Search** page is displayed.

**3.** Click the **New Pattern** button.

Create a pattern, Pattern 1, where:

- Member Type: **User**

- Creation Method: **Multi-bucket**

**4.** Click the **Attribute** tab.

**5.** Click the **Add** icon.

**6.** Select **Time** (Time when the user is logged in) as the attribute.

**7.** Click **Next**.

**8.** Select **For Each** as the **Compare Operator** and 4 as the compare value.

**9.** Press **Add**.

**10.** Click the **Patterns** tab.

**11.** Create a pattern, Pattern 2, where:

- Member Type: **User**

- Creation Method: **Multi-bucket**

**12.** Click the **Attribute** tab.

**13.** Click the **Add** icon.

**14.** Select **State** as the attribute.

15. Select compare operator as for each state.

16. Click **Next**.

17. Create **Rule1**: Add pattern condition, **Entity is member of bucket less than some percentage of times**. (Select Pattern 1 and percentage = 10 and select 1 month as time period.)

18. Add condition to rule, **User: Question status to check if he has registered questions.**

19. Add action, **KBA Challenge** to Rule 1." (This rule triggers if the user has registered questions and he has logged in from time bucket less than 10% of time. The Result, he is challenged with KBA).

20. Create **Rule 2**: Add pattern condition, **Entity is member of bucket less than some percentage of times**. (Select Pattern 2, percentage =20 and select 15 days as time period)

21. Create **Rule 3**: Add pattern condition, **User: Is OTP enabled**. (Using condition **Challenge Channel Status**)

22. Create a policy and add all three rules.

23. Add trigger combination to policy such that if all rules are triggering (true) then action is **Challenge OTP**.

For more information on patterns, see Chapter 17, "Managing Autolearning."

## 10.34.9 Use Case: Configuring User Flow

Jeff a Security Administrator has a brand new installation and must import the base security policies into the development environment of the Oracle Adaptive Access Manager Server. To support the base policies he also configures a black-listed country group. As well he links user groups to the proper roll-out phase policies to test phase two for a group of test users.

To import a policy:

1. Log in to OAAM Admin as an administrator.

2. In the Navigation tree, double-click **Policies**. The **Policies Search** page is displayed.

3. Click **Import Policy** in the **Policies Search** page. The **Import Policy** screen is displayed.

4. Click **Browse** and search for **oaam_sample_policies_for_uio_integration.zip**.

5. Click **OK** to upload **oaam_sample_policies_for_uio_integration.zip**.

   A confirmation dialog displays the status of the operation.

   The imported policies are listed in the **Imported List** section.

   An error is displayed if you try to import files in an invalid forma or an empty ZIP file.

6. Click **OK** to dismiss the confirmation dialog.

7. In the **Policy Search** page, verify that the policy appears in the **Search Results** table.

8. In the Navigation tree, double-click **Groups**. The **Groups Search** page is displayed.

**9.** From the **Groups Search** page, click the **New Group** button or icon.

The **New Group** screen is displayed.

You could also open the **New Group** screen by right-clicking **Group** in the Navigation tree and selecting **Create** from the context menu that appears.

**10.** In the **New Group** screen, enter **Black-listed Country Group** as the name and provide a description.

**11.** From the **Group Type** list, select **Countries**.

**12.** Set the cache policy to **Full Cache** or **None**.

**13.** Click **OK** to create the **Black-listed Country Group**.

**14.** Click **OK** to dismiss the dialog.

The **Group Details** page for the **Black-listed Country Group** is displayed.

**15.** In the **Countries** tab of the **Group Details** page, click **Add**.

The **Add Member** dialog is displayed.

**16.** From the **Available Countries** table, select one or more countries to add to the group.

**17.** Click **Add**.

**18.** Navigate to the **Policies Search** page.

**19.** Search for the Post-Authentication policy.

**20.** In the **Results** table, click the **Post-Authentication policy**.

The **Policy Details** page appears.

**21.** Link the **Test Users** group to the policy.

**22.** In the **Policy Details** page, click the **Rules** tab.

**23.** In the **Rules** tab, click **Add**.

**24.** In the **New Rule** page, enter the rule name as **Location: In Country Group**.

**25.** Click the **Conditions** tab.

**26.** In the **Conditions** page, click **Add**.

The **Add Conditions** page is displayed where you can search for and select the **Location: In Country Group** condition and add it to the rule.

**27.** Click **OK**.

The parameters for the condition are displayed in the bottom subpanel.

**28.** In the parameters area, for **Country in country group**, select the **Blacklisted Country** group and for **Is In Group**, select **True**.

**29.** Click **Save**.

**30.** In the **Results** tab, select **RegisterUserOptional** as the **Action** group.

**RegisterUserOptional** allows the user to opt in or out of selecting a personalized image.

**31.** Click **Apply**.

## 10.34.10 Use Case: Edit Existing Security Policy

Jeff, a Security Administrator wants to change the maximum number of attempts at a challenge question. He must edit a rule parameter to do this.

Best practice is to set the maximum number of failed KBA challenges to one less than the total number of challenge questions each user registers. For example, if all users register for four questions the maximum failures allowed should be three.

To edit an existing Security Policy, follow these steps:

1. Log in to OAAM Admin as an administrator.

2. In the Navigation tree, double-click **Policies**. The **Policies Search** page is displayed.

3. In the **Search Results** table, click **Fraud Blocking**.

4. In the **Rules** tab of the **Policy Details** page, click **Maximum Number of Failed Challenges**.

5. In the **Conditions** tab of the **Rule Details** page, select **User: Challenge Maximum Failures** on the top panel.

   This condition checks to see if the user failed to answer the challenge question for specified number of times.

6. On the bottom panel, change the value of **Number of Failures More than or equal to** so that it is one less than the total number of challenge questions each user registers.

## 10.34.11 Use Case: Policy Set Scoring Engine

Jeff is a Security Administrator who wants the final risk score at each checkpoint to be based on the highest individual policy risk score. To meet this requirement he selects **Maximum** as the scoring engine at the Policy Set level.

1. Log in to OAAM Admin as an administrator.

2. In the Navigation tree, double-click **Policy Set**. The **Policy Set** page is displayed.

3. Click the **Summary** tab.

4. Select **Maximum** from the **Scoring Engine** list.

   The **Maximum Scoring Engine** takes the highest policy score and uses it as the checkpoint score. This scoring engine ignores the policy weights.

5. Click **Apply**.

   A confirmation dialog appears with the message, "Policy Set details updated successfully."

6. Click **OK**.

## 10.34.12 Use Case: Copy Policy

The security team has decided some of the risk evaluations would work better before a user logs in. Jack, a Security Administrator must move a policy from the post-authentication checkpoint to the pre-authentication checkpoint to meet this new requirement. He looks through the rules in this policy to make sure they are all functional with the data available in pre-authentication.

1. Log in to OAAM Admin as an administrator.

2. In the Navigation tree, select **Policies**. The **Policies Search** page is displayed.

3. For the **Checkpoint** filter, select **Post-Authentication** and click **Search**.

4. Look through the policy descriptions in the **Search Results** table for ones that do not occur after the password has been entered and ones that do not use conditions based on challenges.

   The **Fraud Can't Challenge** seems to be one that fits the criteria. The description for **Fraud Can't Challenge** is **Applied to users with no challenge questions active**.

5. Open the **Fraud Can't Challenge** policy to view its rules.

   The rules involve devices, IPs, locations as inputs and there are no actions to challenge the user. Therefore, the policy can be used in the pre-authentication checkpoint.

6. In the **Policy Details** page, click **Copy Policy**.

7. In the **Copy Policy** dialog, select **Pre-Authentication** as the checkpoint.

8. Enter a name and description for the policy.

9. Select **Active** or **Disabled** as the policy status.

   If you want the policy to be enabled as soon as it is created, select **Active** for **Policy Status**.

   If you want to policy to be disabled, select **Disabled**.

   A policy that is disabled is not enforced at the checkpoint.

10. Click **Copy**.

    A copy of the policy is added to the Pre-Authentication checkpoint.

## 10.34.13 Use Case: Conditions: IP: Login Surge

William is a Security Administrator and he must configure a policy and rule to track the number of logins from the same IP and if there are more than 10 logins in 1 hour from an IP, a high alert should be triggered.

1. Log in to OAAM Admin as an administrator.

2. Create a **Monitor IP** group

   a. In the Navigation tree, double-click **Groups**.

   b. In the **Groups Search** page, click the **New Group** button.

      The **Create Group** screen appears.

   c. Enter the group name, **Monitor IPs**, and select **IP** as the **Group type** and click **Create**.

   d. In the **Monitor IPs** group page, click the **IP** tab.

   e. In the **IP** tab, click the **Add** button.

   f. In the **Add IPs** screen, select the **Search and select from the existing IPs** option, enter criteria, then click **Search**.

   g. From the **Search Results** table, select one of the IPs that you want to monitor and click **Add**.

      A confirmation dialog appears.

    **h.** Click **OK**.

    **i.** Add IPs to monitor as needed.

**3.** Create an **IP Surge High Alert** group

    **1.** In the **Groups Search** page, click the **New Group** button.

    The **Create Group** screen appears.

    **2.** Enter the group name, **IP Surge**, and select **Alerts** as the **Group type** and click **Create**.

    A confirmation message appears.

    **3.** Click **OK** to dismiss the confirmation dialog.

    The new **IP Surge alert** group is created successfully and the **Group Details** page is displayed.

    **4.** Click the **Alerts** tab to add alerts to the group.

    **5.** In the **Alerts** tab, click the **Add** (Add Member) button.

    **6.** In the **Add Member** page, select **Create new element**.

    **7.** For **Alert Type**, select **Investigator**.

    **8.** For **Alert Level**, select **High**.

    **9.** For **Alert Message**, enter "More than 10 logins from the same IP in 1 hour."

    **10.** Click **Add** to add the alert to the group.

    A confirmation dialog appears.

    **11.** Click **OK** to dismiss the dialog.

**4.** In the Navigation tree, double-click **Policies**.

**5.** In the **Policies Search** page, click the **New Policy** button.

The **New Policy** page appears. In the **Summary** tab, the default values for the new policy are displayed as follows:

- Policy Status: **Active**

- Checkpoint: **Pre-Authentication**

- Scoring Engine: **Average**

- Weight: **100**

**6.** Create a new pre-authentication security policy.

    **a.** For **Policy Name**, enter **Logins_SameIP**.

    **b.** For **Description**, enter **Track the number of logins from the same IP and if there are more than 10 logins in the last hour from an IP**.

    **c.** Select **Active** as the policy status; otherwise the policy is not enforced at the checkpoint.

    **d.** Enter **Weighted Maximum Score** for the scoring engine and **100** as the weight.

    **e.** Click **Apply**.

    A confirmation dialog displays the status of the operation.

    If you click **Apply** and the required fields are not filled in an error message is displayed.

      **f.** Click **OK** to dismiss the confirmation dialog.

**7.** Configure the policy to run for all users.

    **a.** Click the **Group Linking** tab.

    **b.** For **Run Mode**, select **All Users**.

      Since **All Users** is selected for the run mode, the policy is executed (run) for all users.

      Specifying a run mode is a mandatory step in order for the policy to execute. It enables the policy to execute/run for a set of users or all users. For information, see Section 10.9, "Linking Policy to All Users or a User ID Group."

    **c.** Click **Apply**.

      A confirmation dialog displays the status of the operation.

    **d.** Click **OK** to dismiss the confirmation dialog.

**8.** Create **IP Excessive Use** rule for the policy.

    **a.** Click the **Rules** tab.

    **b.** In the **Rules** tab, click **Add** to add a new rule.

      The **New Rule** page is displayed.

    **c.** In the **Summary** tab, enter **IP Excessive Use** as the rule name.

    **d.** Enter a description for the rule.

    **e.** Select **Active** as the rule status.

    **f.** Add the **Location: IP excessive use** rule condition to create the new rule.

        **a.** To add the **Location: IP excessive use** condition, click the **Conditions** tab.

        **b.** In the **Conditions** tab, click **Add**. The **Add Condition** page appears.

        **c.** Search for the **Location: IP excessive use** condition by entering **IP** in the **Condition Name** field and then clicking **Search**.

        **d.** In the **Search Results** table, select that condition and click **OK**.

        **e.** In the **New Rule/IP** page, select **Location: IP excessive use** in the top panel.

          The bottom panel displays the parameters of the condition.

        **f.** In the bottom panel, modify the parameters.

          Enter **10** for "Number of Users."

          Select **1** for "Within (hours)."

          Enter **0** for "and not used in (days)."

**9.** Create the **Location: IP in Group** rule for the policy.

    **a.** Click the **Rules** tab in the **Policy Details** page.

    **b.** In the **Rules** tab, click **Add** to add a new rule.

      The **New Rule** page is displayed.

    **c.** In the **Summary** tab, enter **IP in Group** as the rule name.

    **d.** Enter a description for the rule.

    **e.** Select **Active** as the rule status.

    **f.** Add the **Location: IP in Group** rule condition to create the new rule.

        **a.** To add the **Location: IP in Group** condition, click the **Conditions** tab.

        **b.** In the **Conditions** tab, click **Add**. The **Add Condition** page appears.

        **c.** Search for the **Location: IP in Group** condition by entering **IP** in the **Condition Name** field and then clicking **Search**.

        **d.** In the **Search Results** table, select that condition and click **OK**.

        **e.** In the **New Rule/IP** page, select **Location: IP in Group** in the top panel.

          The bottom panel displays the parameters of the condition.

        **f.** In the bottom panel, modify the parameters.

          Select **true** for "Is in List."

          Select the **Monitor IPs** group.

**10.** Create a trigger combination in which if both conditions are true, trigger the **Block** action and the **IP Surge Alert.**

    **1.** In the **Policy Details** page, click the **Trigger Combination** tab.

    **2.** Click the **Add** button.

    **3.** For the **IP Excessive Use**, select **True**.

    **4.** For the **IP in Group**, select **True**.

    **5.** For **Action Group**, select **Block**.

    **6.** For **Alert Group**, select **IP Surge High Alert**.

    **7.** Click **Apply**.

## 10.34.14 Use Case: Canceling Rule Creation

William is a Security Administrator and he creates a new policy. He is not sure which rule condition would apply for his business use case. Hence he decides to close the rule without adding any condition.

**1.** Log in to OAAM Admin as an administrator.

**2.** In the Navigation tree, double-click **Policies**.

**3.** In the **Policies Search** page, click the **New Policy** button.

**4.** Create a new policy.

**5.** In the **Policy Details** page, click the **Rules** tab.

**6.** In the **Rules** tab, click **Add** to add a new rule.

    The **New Rule** page is displayed.

**7.** Enter the rule name.

**8.** Enter a description for the rule.

**9.** To add the condition, click the **Conditions** tab.

**10.** In the **Conditions** tab, click **Add**. The **Add Condition** page appears.

**11.** Search for the condition by entering a name into the **Condition Name** field and then clicking **Search**.

**12.** In the **Results** table, select that condition.

13. Click **Cancel**.

   You are not sure which rule condition would apply for your business use case.

14. Click the **Delete** button in the upper-right corner.

   An Unsaved Data Warning dialog appears with the message, "You have unsaved data. Are you sure you want to continue?"

15. Click **Yes**.

   You are returned to the **Rules** page.

16. Click the **Delete** button in the upper-right corner again.

   You are returned to the **Policies Search** page.

17. In the **Search Results** table, click the policy you created.

   The rule has not been created.

## 10.34.15 Use Case: Disable Trigger Combinations

Jim is a Security Administrator. He wants to inactivate his trigger combinations and enable them later, but he does not want to lose his settings.

He can accomplish that by not setting the Score/Policy, Actions, and Alerts for the combinations and they are automatically in disabled state. No action would be taken based on these combinations.

To disable trigger combinations:

1. In the Navigation tree, select **Policies**. The **Policies Search** page is displayed.

2. Search for the policy which you want.

3. Click the policy name to open its **Policy Details** page.

4. Navigate to the **Trigger Combinations** tab.

5. Select **0** as the score or make sure no nested policy is specified.

6. Deselect the actions in the action group lists.

7. Deselect the alert sin the alert group lists.

8. In the **Trigger Combinations** tab, click **Apply** after making all your edits.

## 10.34.16 Use Case: Condition: Evaluate Policy

Jeff has two policies. One of the policies **Policy B** is like a pre-cursor to **Policy A** so this policy should be executed every time, no matter what the other rule evaluations turn out to be. Hence nesting this policy under **Policy A** may not work all the time. (trigger combinations)

So Jeff decides to add a new rule condition to **Policy A** such that it executes **Policy B** every time.

1. Open **Policy A**.

2. In the **Rules** tab of the **Policy Details** page, click the **Add Rule** button.

3. Create a rule, **Rule C**.

4. In the **Condition** tab of the **Rule Details** page, click **Add Condition**.

5. Add **System: Evaluation Policy** condition.

6. In **Trigger Combination**, select **Policy B** as action.

## 10.35 Best Practices

This section outlines some best practices for using policies, rules, and conditions.

### 10.35.1 Adding or Editing Policies/Rules

These general steps outline the process for adding or updating of policies or rules into a production environment:

1. Develop the new rule using your offline system (a separate installation of Oracle Adaptive Access Manager set up for testing or staging).

2. Test the rule to ensure that it is functioning as expected by running predictable data through it using your offline system.

3. When you are satisfied that the policy is functioning as expected, migrate the policy in pre-production where performance testing can be run.

   This is an important step since the new rule, or policy, or both can potentially have a performance impact. For example, if you define a new policy to check that a user was not using an email address that had been used before (ever). If the customer has more than 1 billion records in the database, performing that check against all the records for every transaction has great impact on performance. Therefore, testing the policy under load is important.

4. Only when you are satisfied that your new rule/policy is functioning as expected and does not adversely affect performance should it be migrated into production.

# 11

# OAAM Security and Autolearning Policies

This chapter describes the flows for the main scenarios in authentication and the policies and rules that are shipped with the product as part of the OAAM base snapshot. This chapter also includes autolearning policies that are shipped out of the box.

Policies are also included as separate policy files to import but they require that you import questions, entities, and patterns, and set up autolearning related properties.

## 11.1 Authentication Flow

Figure 11–1 shows the authentication flow of OAAM server when a user logs in to an application that is protected by Oracle Adaptive Access Manager.

*Figure 11–1   Authentication Flow*
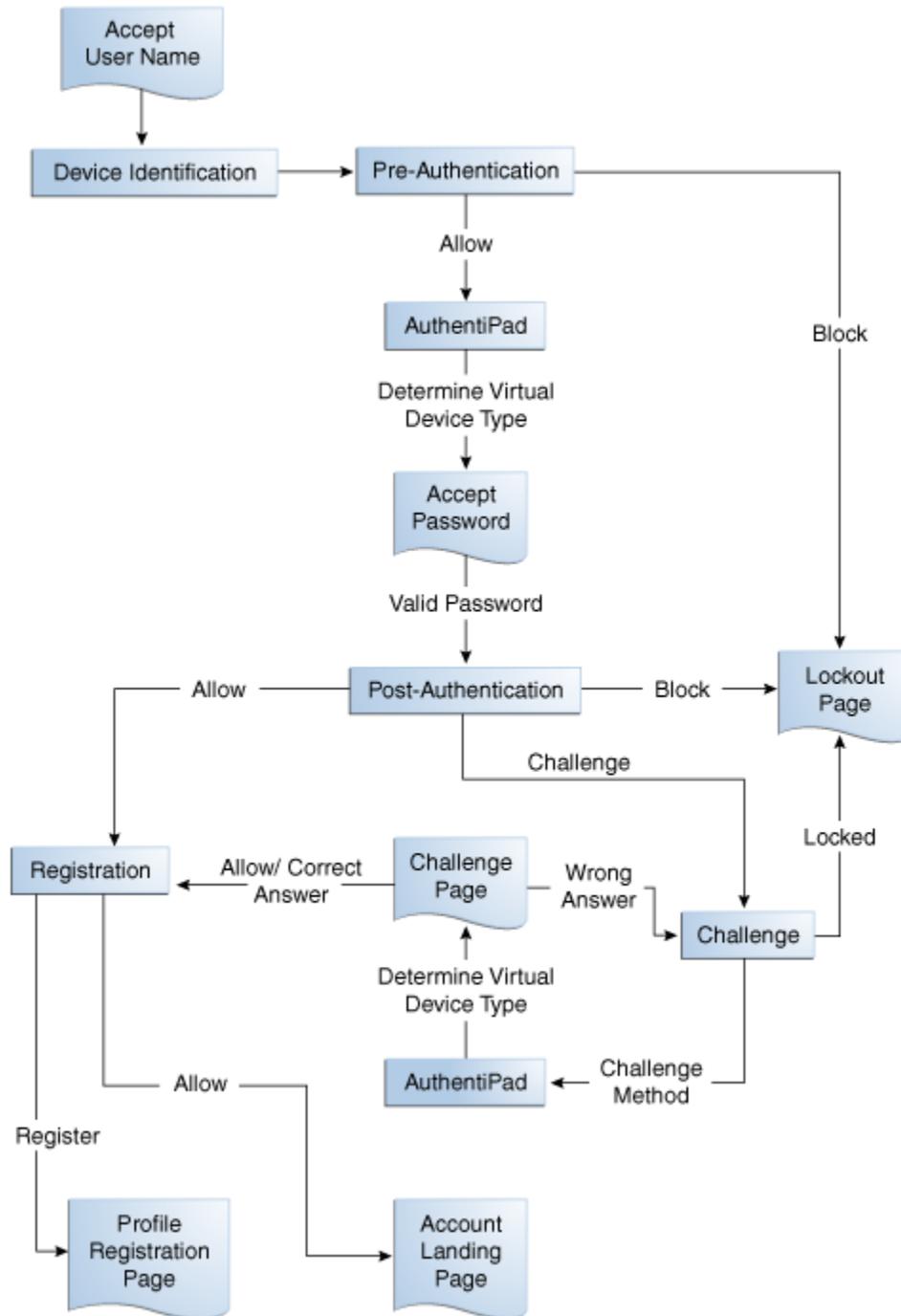


## 11.2  Forgot Password Flow

The Forgot Password flow allows the users to reset their password after successfully answering all challenge questions.

> **Note:** The Forgot Password feature requires Oracle Identity Manager integration.

*Figure 11–2   Forgot Password Flow*
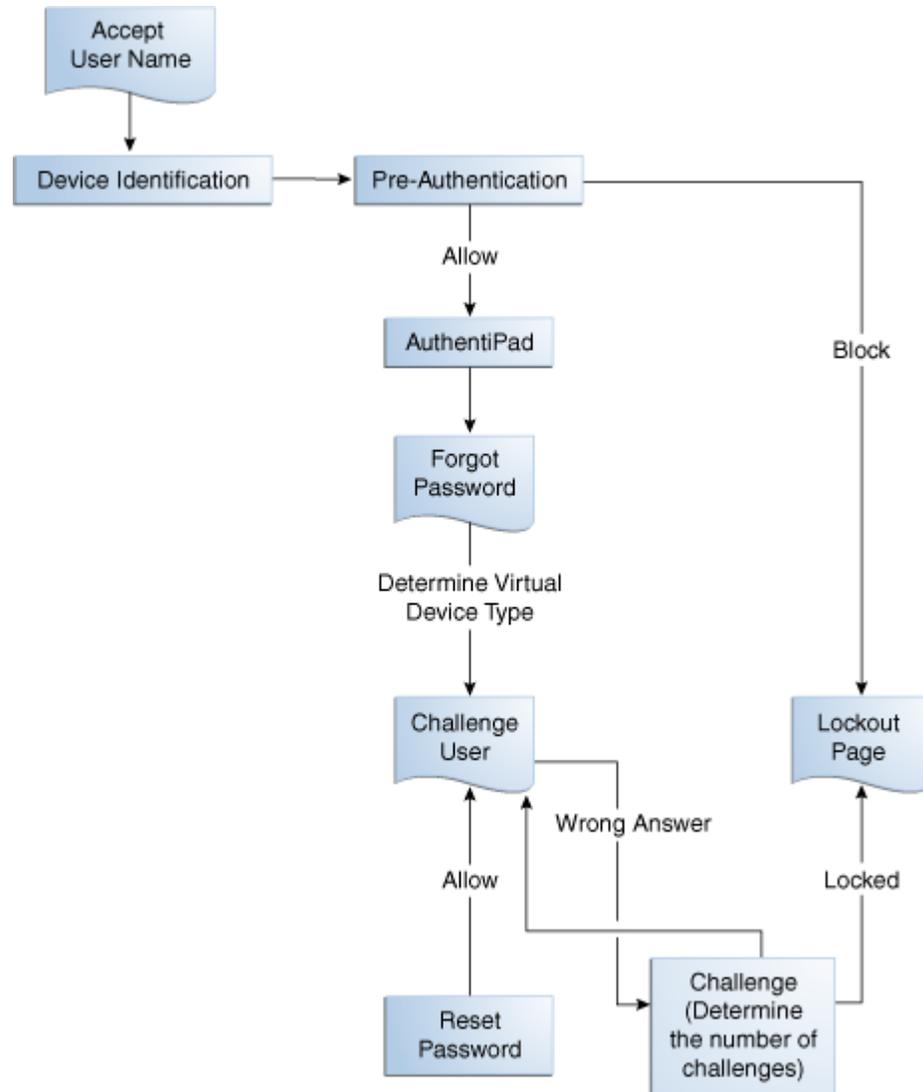


## 11.3 Reset Password (KBA-Challenge) Flow

Challenge Reset enables users to reset their challenge registration.

shows the Reset Password flow.

*Figure 11–3  Reset Password*
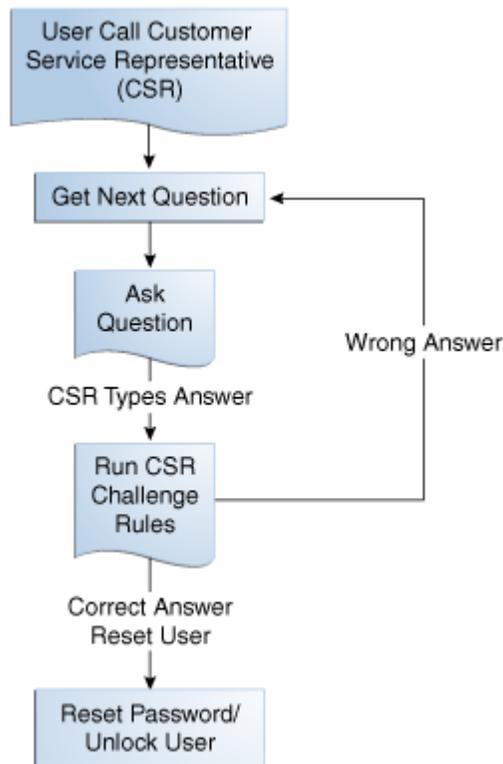
## 11.4  OAAM Checkpoints and Responsibilities

The following table lists the OAAM checkpoints and their responsibilities.

*Table 11–1    OAAM Checkpoints and Responsibilities*

| CheckPoint Name | Responsibilities |
| --- | --- |
| Pre-Authentication | Determine if the request has to be BLOCKED |
| Device Identification | Determine how to identify the device |
| AuthentiPad | Determine which authentication pad to use |
| Post Authentication | Determine if the user has to be ALLOWED or BLOCKED |
| Registration | Determine which pieces of user information is pending registration |
| Challenge | Determine which mechanism to use to challenge the user |
| CSR KBA Challenge | Applicable when customer calls in for service. Reset settings is performed through CSR KBA Challenge. |
| Forgot Password | Activity to reset password performed based on challenge |
| Preferences | Sets the user information (Image, phrase, OTP settings, and so on) |

## 11.5  Out-of-the-Box OAAM Policies

OAAM comes standard with out-of-the-box policies pre-built to detect suspicious activity.

## 11.5.1 OAAM Pre-Authentication

This policy stops fraudulent login attempts before the password is entered.

### 11.5.1.1 Policy Summary

Table 11–2 provides a general summary of the OAAM Pre-Authentication policy.

*Table 11–2    OAAM Pre-Authentication Policy Summary*

| Summary | Details |
| --- | --- |
| Purpose | Stops fraudulent login attempts before the password is entered. |
| Scoring Engine | Maximum |
| Weight | 100 |
| Group Linking | All Users |

### 11.5.1.2 OAAM Pre-Authentication Flow Diagram

Figure 11–4 illustrates the OAAM Pre-Authentication flow.

*Figure 11–4    OAAM Pre-Authentication Flow*
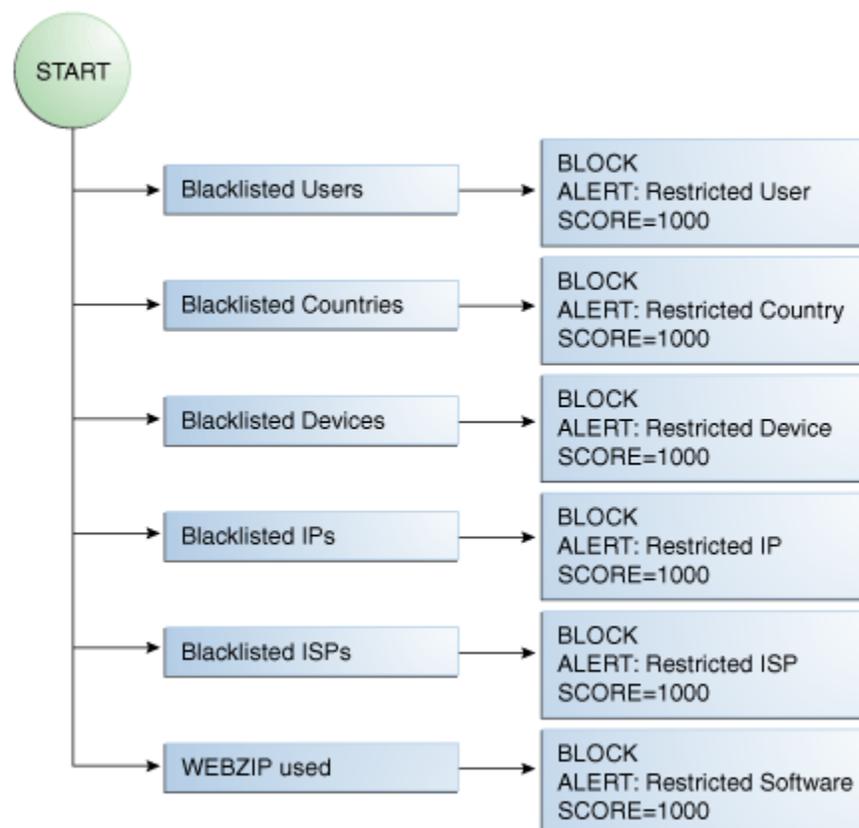


### 11.5.1.3 OAAM Pre-Authentication: Details of Rules

The table below shows the rule conditions and parameters in the OAAM Pre-Authentication Policy.

*Table 11–3    OAAM Pre-Authentication Policy Rules Details*

| Rule | Rule Condition and Parameters | Results |
|---|---|---|
| Blacklisted Countries | **Location: In Country group**<br>Is In List = TRUE<br>Country in country Group=OAAM Restricted Countries | Action = OAAM Block<br>Alert = OAAM Restricted Country<br>Score = 1000<br>Weight = 100 |
| Blacklisted devices | **Device: Device in group**<br>Is in group = TRUE<br>Device in group = OAAM Restricted Devices | Action = OAAM Block<br>Alert = OAAM Restricted Device<br>Score = 1000<br>Weight = 100 |
| WEBZIP used | **Device: Browser header substring**<br>Substring to check = WEBZIP | Action = OAAM Block<br>Alert = OAAM Restricted Software<br>Score =1000<br>Weight = 100 |
| Blacklisted IPs | **Location: IP in group**<br>Is in List = TRUE<br>IP List = OAAM Restricted IPs | Action = OAAM Block<br>Alert = OAAM Restricted IP<br>Score = 1000<br>Weight = 100 |
| Blacklisted ISPs | **Location: ISP in group**<br>Is in List = TRUE<br>ISP List = OAAM Restricted ISPs | Action = OAAM Block<br>Alert = OAAM Restricted ISP<br>Score = 1000<br>Weight = 100 |
| Blacklisted users | **User: In Group**<br>Is in group = TRUE<br>User Group = OAAM Restricted Users | Action = OAAM Block<br>Alert = OAAM Restricted User<br>Score = 1000<br>Weight = 100 |

#### 11.5.1.4  Trigger Combinations

None

## 11.5.2  OAAM AuthenticationPad

This policy determines the OAAM Authentication Pad to use.

#### 11.5.2.1  OAAM AuthenticationPad Policy Summary

Table 11–4 provides a general summary of the OAAM AuthentiPad Policy.

*Table 11–4    OAAM AuthenticationPad Policy Summary*

| Summary | Details |
|---|---|
| Purpose | Determines which OAAM Authentication Pad to use. |
| Scoring Engine | Average |
| Weight | 100 |
| Group Linking | All Users |

### 11.5.2.2 OAAM AuthenticationPad Flow Diagram

Figure 11–5 shows the OAAM AuthentiPad flow.

*Figure 11–5   OAAM AuthenticationPad Flow*
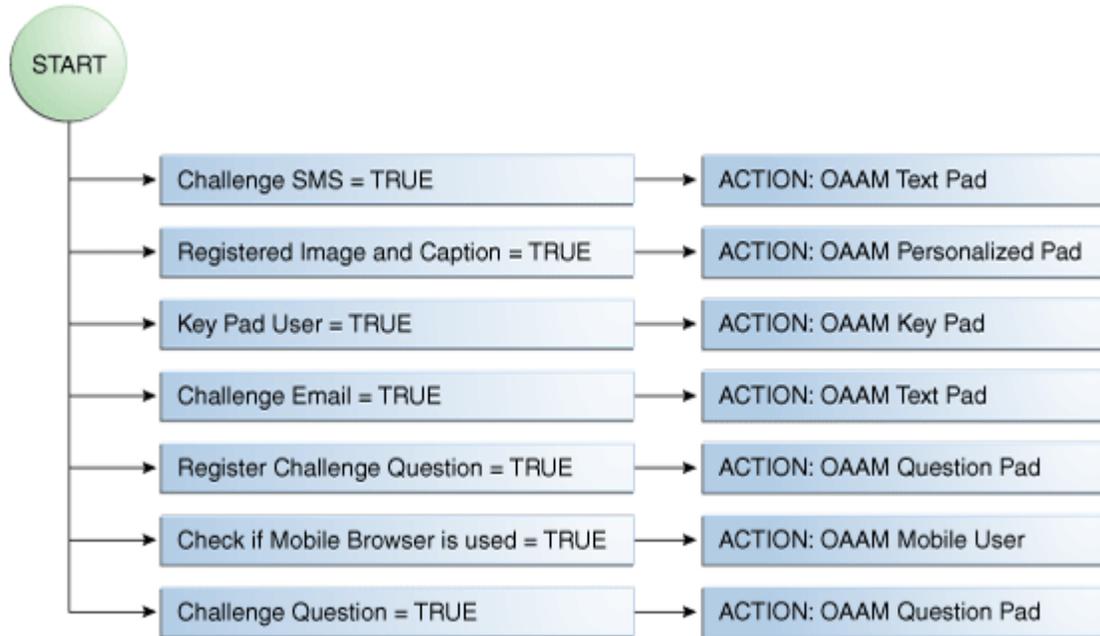


### 11.5.2.3 OAAM AuthenticationPad: Details of Rules

Table 11–5 shows the rule conditions and parameters in the OAAM AuthenticationPad Policy.

*Table 11–5    OAAM Authentication Pad Policy Rules Details*

| Rule | Rule Condition and Parameters | Results |
|---|---|---|
| Challenge SMS | **Session: Check value in comma separated values**<br>Parameter Key = AvailableChallengeTypes<br>Value to Check = ChallengeSMS<br>Return if in list = TRUE | Action = OAAM Text Pad<br>Alert = NONE<br>Score = 0 |
| Registered Image and Caption | **User: Authentication Image Assigned**<br>Is Assigned = TRUE | Action = OAAM Personalized Pad<br>Alert = NONE<br>Score = 0 |
| Key Pad User | **User: Authentication Mode**<br>Authentication Mode is = Full Keypad | Action = OAAM KeyPad<br>Alert = NONE<br>Score = 0 |
| Challenge Email | **Session: Check value in comma separated values**<br>Parameter Key = AvailableChallengeTypes<br>Value to Check = ChallengeEmail<br>Return if in list = TRUE | Action = OAAM Text Pad<br>Alert = NONE<br>Score = 0 |

*Table 11–5   (Cont.)  OAAM Authentication Pad Policy Rules Details*

| Rule | Rule Condition and Parameters | Results |
|---|---|---|
| Register Challenge Question | **Session: Check value in comma separated values**<br><br>Parameter Key = AvailableChallengeTypes<br><br>Value to Check = RegisterChallengeQuestion<br><br>Return if in list = TRUE | Action = OAAM Question Pad<br><br>Alert = NONE<br><br>Score = 0 |
| Check if mobile browser is used | **DEVICE: Check if device is using Mobile Browser**<br><br>Mobile Browsers Group = OAAM Mobile Browsers Group<br><br>Default Return Value = FALSE | Action = NONE<br><br>Alert =OAAM Mobile Users<br><br>Score = 0 |
| Challenge Question | **Session: Check value in comma separated values**<br><br>Parameter Key = AvailableChallengeTypes<br><br>Value to Check = ChallengeQuestion<br><br>Return if in list = TRUE | Action = OAAM Question Pad<br><br>Alert = NONE<br><br>Score = 0 |

### 11.5.2.4  OAAM AuthenticationPad: Trigger Combinations

Table 11–6 describes the OAAM Authentipad trigger combinations.

*Table 11–6    OAAM AuthenticationPad Policy Trigger Combinations*

| Description | Combination Detail | Result |
|---|---|---|
| Empty in the snapshot (Detect Mobile Browser) | **Check if Mobile Browser is Used = TRUE**<br>Challenge SMS = Any<br>Registered Image and Caption =Any<br>Key Pad User = Any<br>Challenge Email = Any<br>Challenge Question = Any<br>Register Challenge Question = Any | **Action = OAAM HTML Pad**<br>Alert = NONE<br>Score = 0 |
| Empty in the snapshot (Unregistered Users) | Check if Mobile Browser is Used = Any<br>Register Challenge Question = Any<br>Challenge SMS = FALSE<br>**Registered Image and Caption = FALSE**<br>Key Pad User = FALSE<br>Challenge Email = FALSE<br>Challenge Question = FALSE | **Action = OAAM Text Pad**<br>Alert = NONE<br>Score = 0 |
| Empty in the snapshot (Registered Users) | Register Challenge Question = Any<br>Check if Mobile Browser is Used = Any<br>Challenge SMS = FALSE<br>**Registered Image and Caption = TRUE**<br>Key Pad User = FALSE<br>Challenge Email = FALSE<br>Challenge Question = FALSE | **Action = OAAM Text Pad Personalized**<br>Alert = NONE<br>Score = 0 |

## 11.5.3 OAAM Post-Authentication Security

This policy evaluates the level of risk after authentication is successful. The possible actions are Allow, Block, or Challenge.

### 11.5.3.1 OAAM Post-Authentication Security Policy Summary

Table 11–7 provides a summary of the Post-Authentication Security Policy.

*Table 11–7  OAAM Post-Authentication Security Policy Summary*

| Summary | Details |
| --- | --- |
| Purpose | Evaluates the level of risk after authentication is successful. The possible actions are Allow, Block, or Challenge. |
| Scoring Engine | Maximum |
| Weight | 100 |
| Group Linking | All Users |

### 11.5.3.2 OAAM Post-Authentication Security Flow Diagram

Figure 11–6 shows the Post-Authentication Security flow.

*Figure 11–6   OAAM Post Authentication Security Flow*



START

| Active Anonymizer | ACTION: OAAM Block<br>ALERT: OAAM Active Anonymizer IP<br>SCORE: 1000 |
| User Blocked Recently | ACTION: OAAM Challenge<br>ALERT: OAAM User Blocked Recently<br>SCORE: 700 |
| Suspect Anonymizer | ACTION: OAAM Challenge<br>ALERT: OAAM Suspect Anonymizer IP<br>SCORE: 700 |
| Unknown Anonymizer | ACTION: OAAM Challenge<br>ALERT: OAAM Unknown Anonymizer IP<br>SCORE: 600 |
| Dormant Device | ACTION: OAAM Challenge<br>ALERT: OAAM Dormant Device<br>SCORE: 500 |
| Risky Countries | ACTION: OAAM Challenge<br>ALERT: OAAM Monitor Country<br>SCORE: 500 |
| Device with Many failures | ACTION: OAAM Challenge<br>ALERT: OAAM Many Failures from Device<br>SCORE: 600 |
| Max Device Per User | ACTION: OAAM Challenge<br>ALERT: OAAM Max Device Per User<br>SCORE: 300 |
| Devices Maximum Velocity | ACTION: OAAM Challenge<br>ALERT: OAAM Device Maximum Velocity<br>SCORE: 700 |
| Risky Connection Type | ACTION: OAAM Challenge<br>ALERT: OAAM Risky Connection Type<br>SCORE: 700 |
| Surge of Users from IP | ACTION: OAAM Challenge<br>ALERT: OAAM IP Multiple Users<br>SCORE: 600 |
| Private Anonymizer | ACTION: OAAM Challenge<br>ALERT: OAAM Private Anonymizer IP<br>SCORE: 700 |
| Maximum Users per Device | ACTION: OAAM Challenge<br>ALERT: OAAM Device Multiple Users<br>SCORE: 500 |
| Risky Device | ACTION: OAAM Challenge<br>ALERT: OAAM Risky Device<br>SCORE: 700 |
| Risky IP | ACTION: OAAM Challenge<br>ALERT: OAAM Risky IP<br>SCORE: 700 |
| Dormant IP | ACTION: OAAM Challenge<br>ALERT: OAAM Dormant IP<br>SCORE: 500 |

### 11.5.3.3 OAAM Post-Authentication Security: Details of Rules

Table 11–8 shows the rule conditions and parameters in the OAAM Post-Authentication Security Policy.

*Table 11–8   OAAM Post Authentication Security Policy Rules Details*

| Rule | Rule Condition and Parameter Values | Results |
|---|---|---|
| Active Anonymizer | **Location: IP in Group**<br>Is in List = TRUE<br>IP in group = anonymizer_active | Action = OAAM Block<br>Alert = OAAM Active Anonymizer IP<br>Score = 1000 |
| Suspect Anonymizer | **Location: IP in Group**<br>Is in List = TRUE<br>IP in group = anonymizer_suspect | Action = OAAM Challenge<br>Alert = OAAM Suspected Anonymizer IP<br>Score = 700 |
| Unknown Anonymizer | **Location: IP in Group**<br>Is in List = TRUE<br>IP in group = anonymizer_active | Action = OAAM Challenge<br>Alert = OAAM Unknown Anonymizer IP<br>Score = 600 |
| Private Anonymizer | **Location: IP in Group**<br>Is in List = TRUE<br>IP in group = anonymizer_private | Action = OAAM Challenge<br>Alert = OAAM Private Anonymizer IP<br>Score = 700 |
| Risky Connection Type | **Location: IP Connection Type in Group**<br>Is in List = TRUE<br>Connection type in group = OAAM High Risk Connection Types | Action = OAAM Challenge<br>Alert = OAAM Risky Connection type<br>Score = 700 |
| User Blocked Recently | **User: Action Timed**<br>Check Action = BLOCK<br>In seconds = 28800<br>More than = 2 | Action = OAAM Challenge<br>Alert = User Blocked Recently<br>Score = 700 |
| Maximum Users per Device | **Device: User Count**<br>Seconds Elapsed = 2592000<br>Max number of users allowed = 5 | Action = OAAM Challenge<br>Alert = OAAM Device Multiple Users<br>Score = 500 |
| Dormant IP | **Location: IP Connection type in group**<br>Is in List = FALSE<br>Connection type group = OAAM Mobile Connections<br>**Location: IP Excessive Use**<br>Number of Users = 4<br>Within (hours) = 24<br>And not used in days = 30 | Action = OAAM Challenge<br>Alert = OAAM Dormant IP<br>Score = 500 |

*Table 11–8   (Cont.)  OAAM Post Authentication Security Policy Rules Details*

| Rule | Rule Condition and Parameter Values | Results |
|------|-------------------------------------|---------|
| Surge of Users from IP | **Location: IP Connection type in group** | Action = OAAM Challenge |
| | Is in List = FALSE | Alert = OAAM IP Multiple Users |
| | Connection type group = OAAM Mobile Connections | Score = 600 |
| | **Location: IP is AOL** | |
| | Is AOL = False | |
| | **Location: IP Maximum Users** | |
| | Seconds Elapsed = 300 | |
| | Max number of users = 3 | |
| Risky countries | **Location: In Country Group** | Action = OAAM Challenge |
| | Is in List = TRUE | Alert = OAAM Monitored Country |
| | Country in country group = OAAM Monitoring Countries | Score = 500 |
| Dormant Device | **Device: Excessive Use** | Action = OAAM Challenge |
| | Number of Users = 4 | Alert = OAAM Dormant Device |
| | Within (hours) = 24 | Score = 500 |
| | And not used in (days) = 30 | |
| Device with Many Failures | **Device: Timed not status** | Action = OAAM Challenge |
| | Authentication status is not = SUCCESS | Alert = OAAM Many Failures from Device |
| | Within duration (seconds) = 28800 | Score =600 |
| | For more than 4 (times) | |
| Maximum Devices per User | **User: Check Devices Used** | Action = OAAM Challenge |
| | Maximum number of devices = 2 | Alert = OAAM Max Devices for User |
| | Within duration (seconds) = 28800 | Score =300 |
| Risky Device | **Device: In List** | Action = OAAM Challenge |
| | Is in group= TRUE | Alert = OAAM Risky Device |
| | Device in group = OAAM Risky Devices | Score = 700 |
| Device Maximum Velocity | **Device: Velocity from last login** | Action = OAAM Challenge |
| | Last Login within (Seconds) = 72000 | Alert = OAAM Device Maximum Velocity |
| | Miles per Hour is more than = 600 | Score =700 |
| Risky IP | **Location: IP in group** | Action = OAAM Challenge |
| | Is in List = TRUE | Alert = OAAM Risky IP |
| | IP List = OAAM Risky IPs | Score = 700 |

### 11.5.3.4  OAAM Post-Authentication Security: Trigger Combinations

None

## 11.5.4  OAAM Predictive Analysis

This policy harnesses the predictive capabilities of Oracle Data Miner. The rules in this policy are only functional if Oracle Data Miner is configured.

### 11.5.4.1  OAAM Predictive Analysis Policy Summary

Table 11–9 provides a summary of the OAAM Predictive Analysis Policy.

*Table 11–9    OAAM Predictive Analysis Policy Summary*

| Summary | Details |
|---------|---------|
| Purpose | Harnesses the predictive capabilities of Oracle Data Miner. These rules are only functional if Oracle Data Miner is configured. |
| Scoring Engine | Maximum |
| Weight | 100 |
| Group Linking | Linked Users |

### 11.5.4.2  OAAM Predictive Analysis Flow Diagram

Figure 11–7 shows the OAAM Predictive Analysis flow.

*Figure 11–7    OAAM Predictive Analysis Policy Flow*
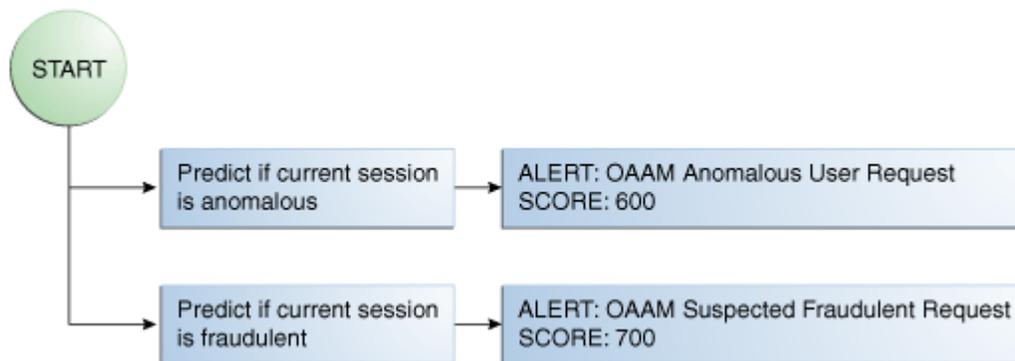


### 11.5.4.3  OAAM Predictive Analysis Policy: Details of Rules

Table 11–10 shows the rule conditions and parameters in the OAAM Predictive Analysis Policy.

*Table 11–10    OAAM Predictive Analysis Policy Rules Details*

| Rule | Rule Condition and Parameters | Results |
|------|-------------------------------|---------|
| Predict if current session is fraudulent | **USER: Check Fraudulent User Request**<br>Classification Model = OAAM Fraud Request Model<br>Required Classification = Fraud<br>Minimum Value of Probability required = 0.70<br>Maximum Value of Probability required = 1.00<br>Default Value to return if error = FALSE | Action = NONE<br>Alert = OAAM Suspected Fraudulent request<br>Score = 700 |
| Predict if current session is anomalous | **USER: Check Anomalous User Request**<br>Anomaly Model = OAAM Anomalous Request Model<br>Minimum Value of Probability required = 0.60<br>Maximum Value of Probability required = 1.00<br>Default Value to return if error = FALSE | Action = NONE<br>Alert = OAAM Anomalous Request<br>Score = 600 |

#### 11.5.4.4 OAAM Predictive Analysis Policy: Trigger Combination

None

## 11.5.5 Auto-learning (Pattern-Based) Policy: OAAM Does User Have Profile

This policy checks if pattern autolearning is enabled and if a user has past behavior recorded. Users with enough recorded behavior are evaluated against their own profile while users without enough recorded behavior are evaluated against the profiles of all other users.

#### 11.5.5.1 OAAM Does User Have Profile Policy Summary

Table 11–11 provides a summary of the OAAM Does User Have Profile Policy.

*Table 11–11   Auto-learning (Pattern-Based) Policy: OAAM Does User Have Profile Summary*

| Summary | Details |
| --- | --- |
| Purpose | Checks if pattern autolearning is enabled and if a user has past behavior recorded. Users with enough recorded behavior are evaluated against their own profile while users without enough recorded behavior are evaluated against the profiles of all other users. |
| Scoring Engine | Maximum |
| Weight | 100 |
| Group Linking | All Users |

#### 11.5.5.2 OAAM Does User Have Profile Flow Diagram

Figure 11–8 shows the OAAM Does User Have Profile flow.

*Figure 11–8   Autolearning (Pattern-Based) Policy: OAAM Does User Have Profile Flow*
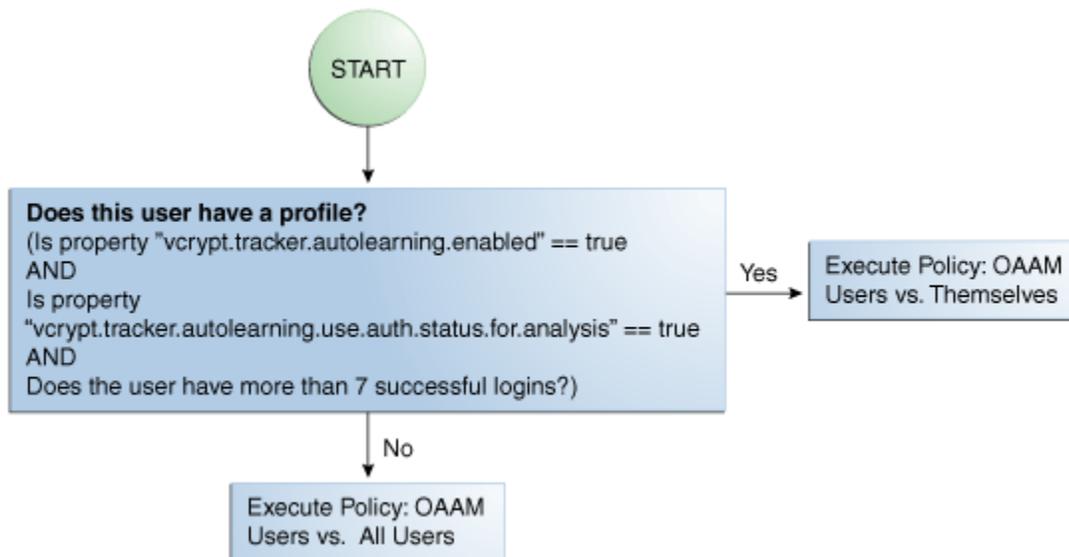


#### 11.5.5.3 OAAM Does User Have Profile: Details of Rules

Table 11–12 shows the rule conditions and parameters in the OAAM Does User Have Profile Policy.

*Table 11–12  Auto-learning (Pattern-Based) Policy Rules Details: OAAM Does User Have Profile*

| Rule | Rule Condition and Parameters | Results |
|---|---|---|
| Does user have a profile | **System - Check Boolean Property** | Action = None |
| | Property = vcrypt.tracker.autolearning.enabled | Alert = None |
| | Value = True | Score = 0 |
| | Default Return Value = True | |
| | **System - Check Boolean Property** | |
| | Property = vcrypt.tracker.autolearning.use.auth.status.for.analysis | |
| | Value = True | |
| | Default Return Value = False | |
| | **User - Check Login Count** | |
| | Check only current user = True | |
| | Authentication Status = Success | |
| | In seconds = 0 | |
| | With Login more than = 7 | |
| | If Error return = False | |
| | Consider current request or not = True | |

### 11.5.5.4  OAAM Does User Have Profile: Trigger Combination

Table 11–13 describes the OAAM Does User Have Profile trigger combinations.

*Table 11–13  Auto-learning (Pattern-Based) Policy: OAAM Does User Have Profile Trigger Combination*

| Description | Combination Detail | Result |
|---|---|---|
| If a user has enough recorded behavior in his profile he is evaluated by this policy. | **Does User have profile = TRUE** | **Policy = OAAM users vs. themselves**<br>Alert = NONE |
| If a user does not have enough recorded behavior in his profile he is evaluated by this policy. | **Does User have profile = ANY** | **Policy = OAAM users vs. all users**<br>Alert = NONE |

## 11.5.6  Auto-learning (Pattern-Based) Policy: OAAM Users vs. Themselves

If a user has a sufficient amount of historical data captured, this policy is used to evaluate his current behavior against his own historical behavior. This policy uses pattern-based rules to evaluate risk.

### 11.5.6.1  OAAM Users vs. Themselves Policy Summary

Table 11–14 provides a summary of the OAAM Users vs. Themselves Policy.

*Table 11–14  Auto-learning (Pattern-Based) Policy: OAAM Users vs. Themselves Summary*

| Summary | Details |
|---|---|
| Purpose | Used to evaluate a user's current behavior against his own historical behavior. This policy uses pattern-based rules to evaluate risk. |
| Scoring Engine | Maximum |
| Weight | 100 |
| Group Linking | Linked Users (It is a nested policy) |

### 11.5.6.2 OAAM Users vs. Themselves Flow Diagram

Figure 11–9 shows the OAAM Users vs. Themselves flow.

*Figure 11–9   Auto-learning (Pattern-Based) Policy: OAAM Users vs. Themselves Flow*
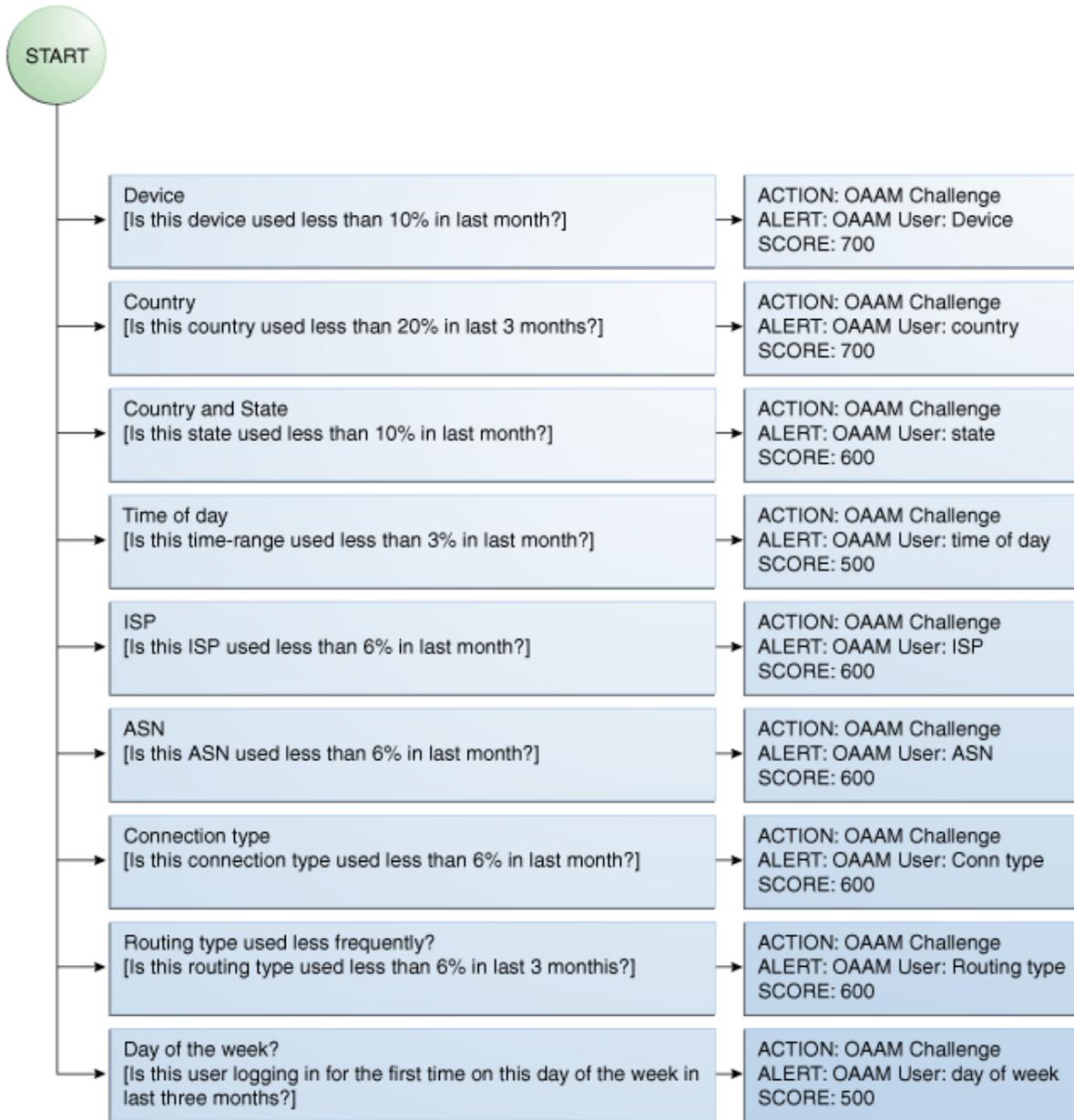


### 11.5.6.3 OAAM Users vs. Themselves: Details of Rules

Table 11–15 shows the rule conditions and parameters in the OAAM Users vs. Themselves Policy.

*Table 11–15    Auto-learning (Pattern-Based) Policy Rules Details: OAAM Users vs. Themselves*

| Rule | Rule Condition and Parameters | Results |
|---|---|---|
| ISP | **ENTITY: Entity is member of pattern less than some percent times**<br>Pattern Hit Percent less than = 6<br>Pattern name for membership = User: ISP profiling pattern<br>Is Membership Count Less than patternHitPercent = True<br>Time period type for pattern membership = Months<br>Time period for pattern membership = 1<br>Member type for pattern membership = User | Action = OAAM Challenge<br>Alert = OAAM User: ISP<br>Score = 600 |
| Connection type | **ENTITY: Entity is member of pattern less than some percent times**<br>Pattern Hit Percent less than = 6<br>Pattern name for membership = User: ASN profiling pattern<br>Is Membership Count Less than patternHitPercent = True<br>Time period type for pattern membership = Months<br>Time period for pattern membership = 1<br>Member type for pattern membership = User | Action = OAAM Challenge<br>Alert = OAAM User: connection type<br>Score = 600 |
| Routing type | **ENTITY: Entity is member of pattern less than some percent times**<br>Pattern Hit Percent less than = 6<br>Pattern name for membership = User: Routing type profiling pattern<br>Is Membership Count Less than patternHitPercent = True<br>Time period type for pattern membership = Months<br>Time period for pattern membership = 1<br>Member type for pattern membership = User | Action = OAAM Challenge<br>Alert = OAAM User: Routing type<br>Score = 600 |
| Device | **ENTITY: Entity is member of pattern less than some percent times**<br>Pattern Hit Percent less than = 10<br>Pattern name for membership = User: Device profiling pattern<br>Is Membership Count Less than patternHitPercent = True<br>Time period type for pattern membership = Months<br>Time period for pattern membership = 1<br>Member type for pattern membership = User | Action = OAAM Challenge<br>Alert = OAAM User: Device<br>Score = 700 |
| Day of the week | **ENTITY: Entity is member of pattern bucket for first time in certain time period**<br>Pattern name for membership = User: Day of Week profiling pattern<br>Is ConditionTrue = True<br>Time period type for pattern membership = Months<br>Time period for pattern membership = 3<br>Member type for pattern membership = User<br>First time count = 1 | Action = OAAM Challenge<br>Alert = OAAM User: day of the week<br>Score = 500 |

*Table 11–15   (Cont.)  Auto-learning (Pattern-Based) Policy Rules Details: OAAM Users vs. Themselves*

| Rule | Rule Condition and Parameters | Results |
|------|-------------------------------|---------|
| Country and State | **ENTITY: Entity is member of pattern less than some percent times**<br><br>Pattern Hit Percent less than = 10<br><br>Pattern name for membership = User: State profiling pattern<br><br>Is Membership Count Less than patternHitPercent = True<br><br>Time period type for pattern membership = Months<br><br>Time period for pattern membership = 1<br><br>Member type for pattern membership = User | Action = OAAM Challenge<br><br>Alert = OAAM User: state<br><br>Score = 600 |
| Time of Day | **ENTITY: Entity is member of pattern less than some percent times**<br><br>Pattern Hit Percent less than = 3<br><br>Pattern name for membership = User: time range profiling pattern<br><br>Is Membership Count Less than patternHitPercent = True<br><br>Time period type for pattern membership = Months<br><br>Time period for pattern membership = 1<br><br>Member type for pattern membership = User | Action = OAAM Challenge<br><br>Alert = OAAM User: time of day<br><br>Score = 500 |
| ASN | **ENTITY: Entity is member of pattern less than some percent times**<br><br>Pattern Hit Percent less than = 6<br><br>Pattern name for membership = User: ASN profiling pattern<br><br>Is Membership Count Less than patternHitPercent = True<br><br>Time period type for pattern membership = Months<br><br>Time period for pattern membership = 1<br><br>Member type for pattern membership = User | Action = OAAM Challenge<br><br>Alert = OAAM User: ASN<br><br>Score = 600 |
| Country | **ENTITY: Entity is member of pattern less than some percent times**<br><br>Pattern Hit Percent less than = 20<br><br>Pattern name for membership = User: Country profiling pattern<br><br>Is Membership Count Less than patternHitPercent = True<br><br>Time period type for pattern membership = Months<br><br>Time period for pattern membership = 3<br><br>Member type for pattern membership = User | Action = OAAM Challenge<br><br>Alert = OAAM User: Country<br><br>Score = 700 |

### 11.5.6.4  OAAM Users vs. Themselves: Trigger Combinations

None

## 11.5.7  Autolearning (Pattern-Based) Policy: OAAM Users vs. All Users

If a user does not have a sufficient amount of historical data captured this policy is used to evaluate his current behavior against the historical behavior of all other users. This policy uses pattern-based rules to evaluate risk.

### 11.5.7.1  OAAM Users vs. All Users Policy Summary

Table 11–16 provides a summary of the OAAM Users vs. All Users Policy.

*Table 11–16    Auto-learning (Pattern-Based) Policy: OAAM users vs. All Users Summary*

| Summary | Details |
| --- | --- |
| Purpose | Evaluates the user's current behavior against the historical behavior of all other users. This policy uses pattern-based rules to evaluate risk. |
| Scoring Engine | Maximum |
| Weight | 100 |
| Group Linking | Linked Users (It is a nested policy) |

### 11.5.7.2  OAAM Users vs. All Users Flow Diagram

Figure 11–10 shows the OAAM Users vs. All Users flow.

*Figure 11–10    Auto-learning (Pattern-Based) Policy: OAAM Users vs. All Users Flow*
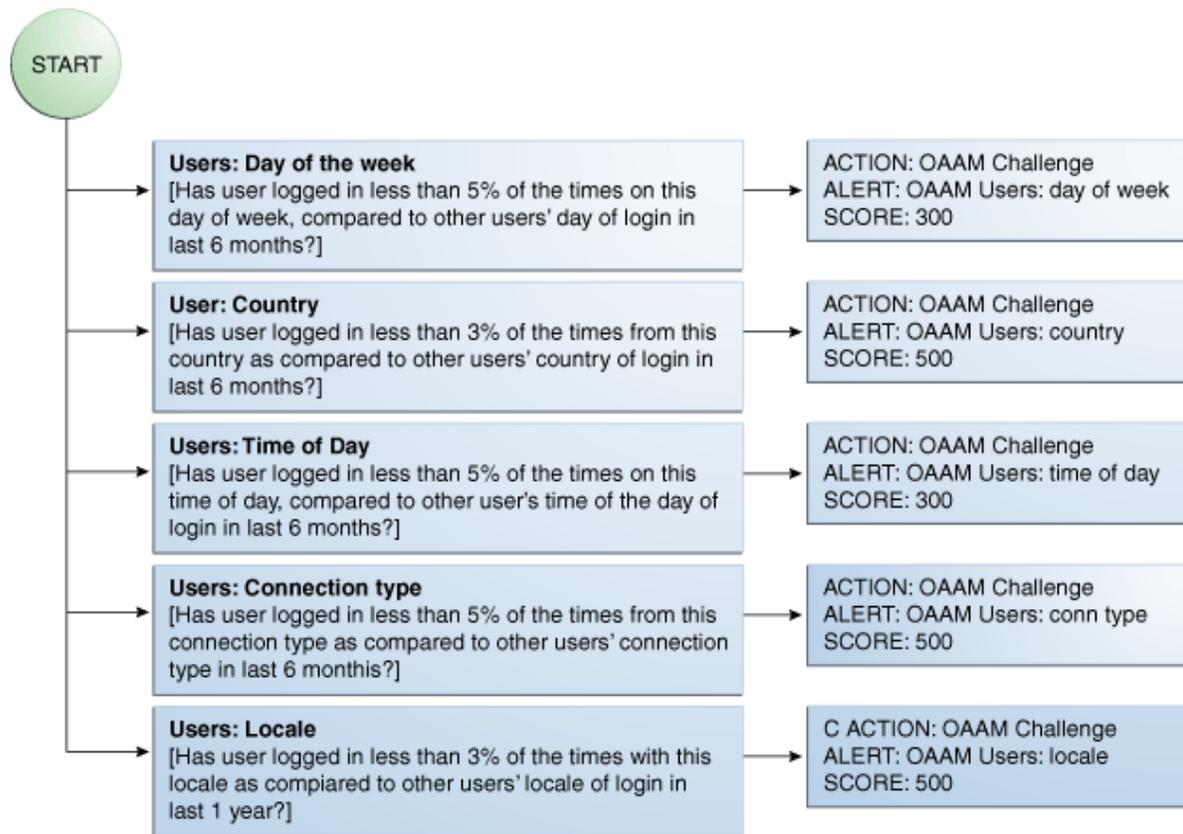


### 11.5.7.3  OAAM Users vs. All Users: Details of Rules

Table 11–17 shows the rule conditions and parameters in the OAAM Users vs. All Users Policy.

*Table 11–17    Auto-learning (Pattern-Based) Policy Rules Details: OAAM Users vs. All User*

| Rule | Rule Condition and Parameters | Results |
|---|---|---|
| Users: Day of the week | **ENTITY: Entity is member of pattern bucket less than some percent with all entities in picture** <br><br> Pattern Bucket Hit Percent less than = 5 <br><br> Pattern name for membership= User: Day of the week profiling pattern <br><br> Is membership count less than pattern hit percent = true <br><br> Time period type for pattern membership = Months <br><br> Time period for pattern membership = 6 <br><br> Member Type for pattern membership = User | Action = OAAM Challenge <br><br> Alert = Users: Day of the week <br><br> Score = 300 |
| Users: Country | **ENTITY: Entity is member of pattern bucket less than some percent with all entities in picture** <br><br> Pattern Bucket Hit Percent less than = 3 <br><br> Pattern name for membership= User: Country profiling pattern <br><br> Is membership count less than pattern hit percent = true <br><br> Time period type for pattern membership = Months <br><br> Time period for pattern membership = 6 <br><br> Member Type for pattern membership = User | Action = OAAM Challenge <br><br> Alert = Users: Country <br><br> Score = 500 |
| Users: Time of Day | **ENTITY: Entity is member of pattern bucket less than some percent with all entities in picture** <br><br> Pattern Bucket Hit Percent less than = 5 <br><br> Pattern name for membership= User: Time of day profiling pattern <br><br> Is membership count less than pattern hit percent = true <br><br> Time period type for pattern membership = Months <br><br> Time period for pattern membership = 6 <br><br> Member Type for pattern membership = User | Action = OAAM Challenge <br><br> Alert = Users: Time of day <br><br> Score = 300 |
| Users: Connection type | **ENTITY: Entity is member of pattern bucket less than some percent with all entities in picture** <br><br> Pattern Bucket Hit Percent less than = 5 <br><br> Pattern name for membership= User: Connection type profiling pattern <br><br> Is membership count less than pattern hit percent = true <br><br> Time period type for pattern membership = Months <br><br> Time period for pattern membership = 6 <br><br> Member Type for pattern membership = User | Action = OAAM Challenge <br><br> Alert = Users: Connection type <br><br> Score = 500 |

*Table 11–17   (Cont.)  Auto-learning (Pattern-Based) Policy Rules Details: OAAM Users vs. All User*

| Rule | Rule Condition and Parameters | Results |
|---|---|---|
| Users: Locale | **ENTITY: Entity is member of pattern bucket less than some percent with all entities in picture** | Action = OAAM Challenge |
| | Pattern Bucket Hit Percent less than = 3 | Alert = Users: Locale |
| | Pattern name for membership= User: Time of day profiling pattern | Score = 500 |
| | Is membership count less than pattern hit percent = true | |
| | Time period type for pattern membership = Years | |
| | Time period for pattern membership = 6 | |
| | Member Type for pattern membership = User | |

### 11.5.7.4  OAAM Users vs. All Users: Trigger Combinations

None

## 11.5.8  OAAM Registration

This policy is used to determine the user information that needs to be registered.

### 11.5.8.1  OAAM Registration Policy Summary

Table 11–18 provides a summary of the OAAM Registration Policy.

*Table 11–18    OAAM Registration Policy Summary*

| Summary | Details |
|---|---|
| Purpose | Determines what parts of user information has to be registered |
| Scoring Engine | Weighted Average |
| Weight | 100 |
| Group Linking | All Users |

### 11.5.8.2  OAAM Registration Flow Diagram

Figure 11–11 shows the OAAM Registration flow.

*Figure 11–11    OAAM Registration Flow*
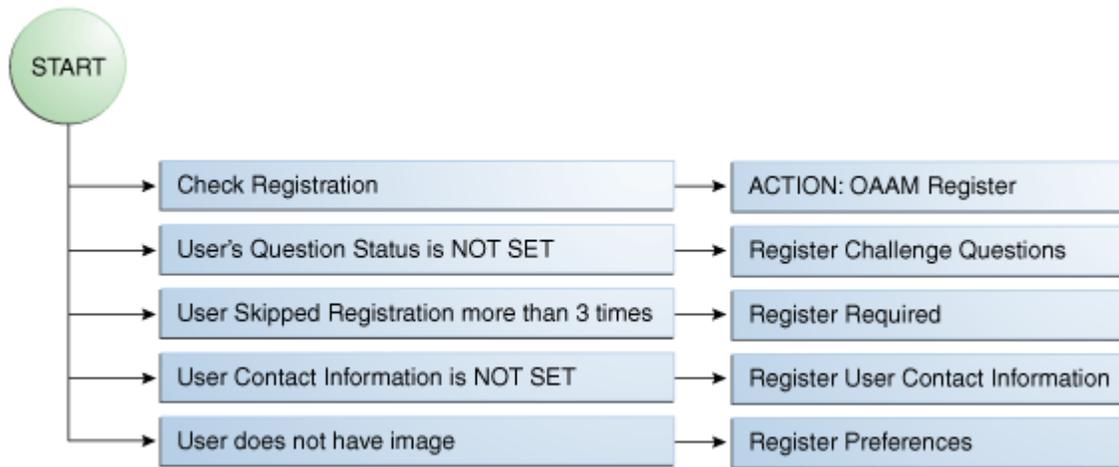


### 11.5.8.3  OAAM Registration: Details of Rules

Table 11–19 shows the rule conditions and parameters in the OAAM Registration Policy.

*Table 11–19    OAAM Registration Policy Rules Details*

| Rule | Rule Condition and Parameters | Results |
| --- | --- | --- |
| Check Registration | **User: Account Status**<br>User Account Status = ACTIVE<br>Is = FALSE | Action = OAAM Register<br>Alert = NONE<br>Score = 0 |
| Register Questions | **User: Question Status**<br>User Question Status = Set<br>Is = FALSE | Action = OAAM Register Challenge Questions<br>Alert = NONE<br>Score = 0 |
| Skipped registration more than 3 times | **User: Action Count Timed**<br>Checkpoint (Optional) = NONE<br>Action = Register User Optional<br>In seconds = 300<br>Count Action only once per session? = TRUE<br>More Than = 3 | Action = OAAM Registration Required<br>Alert = NONE<br>Score = 0 |
| Register User Information | **User: Check Information**<br>Key to comma separated values to check = RequiredChallengeInfo<br>If Information is set, return = FALSE | Action = OAAM Register User Information<br>Alert = NONE<br>Score = 0 |
| Register Image and Caption | **User: Authentication Image Assigned**<br>Is Assigned = FALSE | Action = OAAM Register Preferences<br>Alert = NONE<br>Score = 0 |

### 11.5.8.4  OAAM Registration: Trigger Combinations

None

## 11.5.9  OAAM Challenge

This policy determines how the user has to be challenged. All the decision making in this policy is achieved using trigger combinations.

### 11.5.9.1  OAAM Challenge Policy Summary

Table 11–20 provides a summary of the OAAM Challenge Policy.

*Table 11–20    OAAM Challenge Policy Summary*

| Summary | Details |
| --- | --- |
| Purpose | Determines how the user has to be challenged. All the decision making in this policy is achieved using trigger combinations. |
| Scoring Engine | Weighted Average |
| Weight | 100 |
| Group Linking | All Users |

### 11.5.9.2  OAAM Challenge Flow Diagram

Figure 11–12 shows the OAAM Challenge flow.

*Figure 11–12   OAAM Challenge Flow*
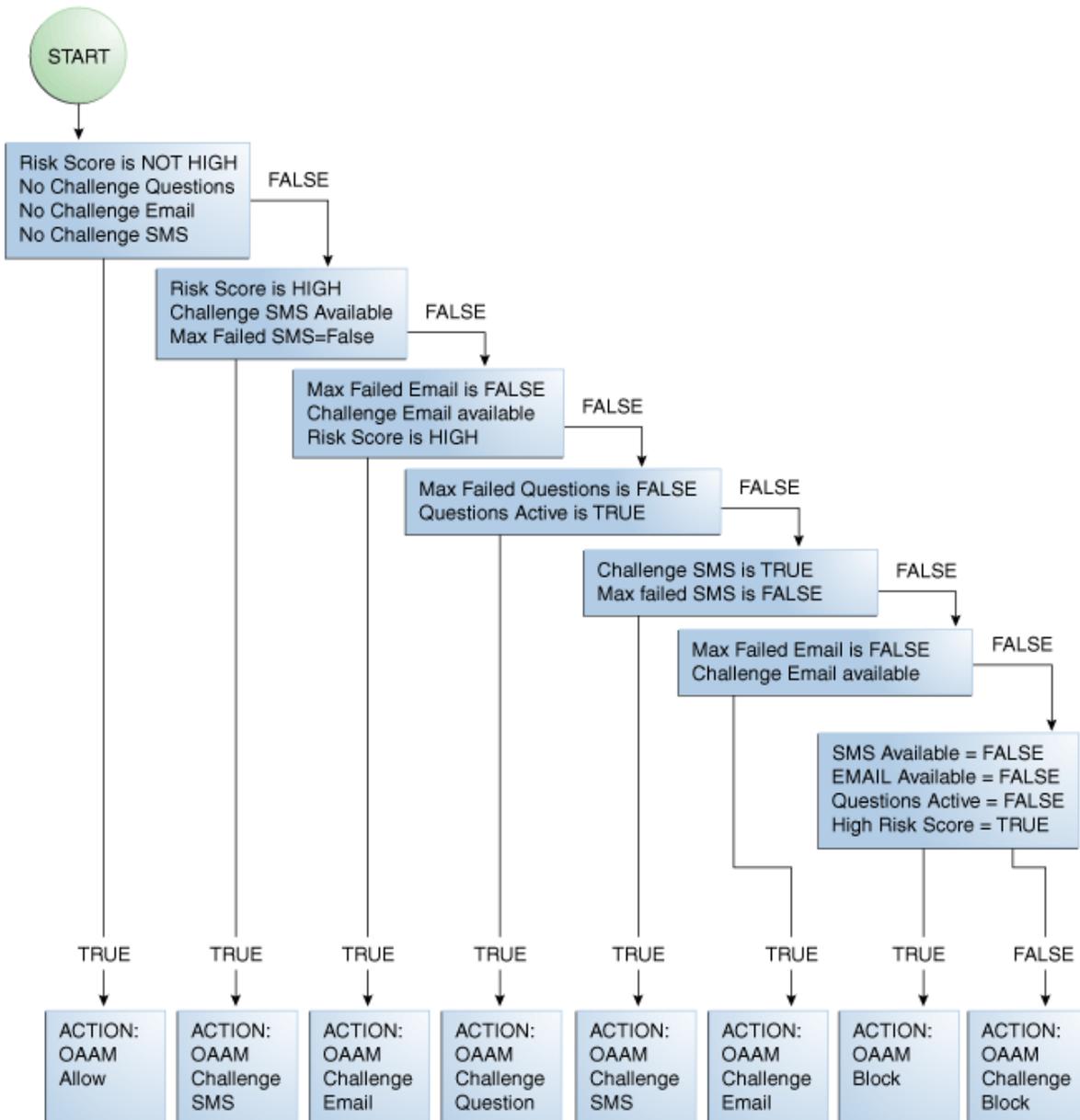


### 11.5.9.3  OAAM Challenge: Details of Rules

Table 11–21 shows the rule conditions and parameters in the OAAM Challenge Policy.

*Table 11–21   OAAM Challenge Policy Rules Details*

| Rule | Rule Condition and Parameters | Results |
|---|---|---|
| Max failed SMS attempts | **User: Check OTP failures**<br>OTP Challenge Type = ChallengeSMS<br>Failure More than or Equal To = 3<br>If above or equal = TRUE | Action = NONE<br>Alert = NONE<br>Score = 0 |
| Max failed Email attempts | **User: Check OTP failures**<br>OTP Challenge Type = ChallengeEmail<br>Failure More than or Equal To = 3<br>If above or equal = TRUE | Action = NONE<br>Alert = NONE<br>Score = 0 |
| Max failed Question attempts | **User: Challenge Maximum Failures**<br>Number of Failures More than or equal to = 3<br>Current Question Count only? = False<br>If above or equal, return = True | Action = NONE<br>Alert = NONE<br>Score = 0 |
| Questions Active | **User: Question Status**<br>User Question Status = Set<br>Is = True | Action = NONE<br>Alert = NONE<br>Score = 0 |
| Challenge Email Available | **Session: Check value in comma separated values**<br>Parameter Key = AvailableChallengeTypes<br>Value to Check = ChallengeEmail<br>Return if in list = True | Action = NONE<br>Alert = NONE<br>Score = 0 |
| Challenge SMS Available | **Session: Check value in comma separated values**<br>Parameter Key = AvailableChallengeTypes<br>Value to Check = ChallengeSMS<br>Return if in list = True | Action = NONE<br>Alert = NONE<br>Score = 0 |
| Check for HIGH Risk Score | **Session: Check Risk Score Classification**<br>Risk score classification to check = High Risk<br>Default value to return in case of errors = False | Action = NONE<br>Alert = NONE<br>Score = 0 |

### 11.5.9.4  OAAM Challenge: Trigger Combinations

Table 11–22 describes the OAAM Challenge trigger combinations.

*Table 11–22    OAAM Challenge Trigger Combinations*

| Description | Combination Detail | Result |
| --- | --- | --- |
| Allow the user to register if the risk score is not High and if the user is not registered | **Check for High Risk Score = False**<br>**Questions Active = False**<br>**Challenge Email Available = False**<br>**Challenge SMS Available = False**<br>Max failed Question Attempts = Any<br>Max failed Email Attempts = Any<br>Max failed SMS Attempts = Any | Policy = NONE<br>**Action = OAAM Allow**<br>Alert = NONE<br>Score = 0 |
| Challenge the user with SMS if the risk score is High and he is registered for SMS and has not failed the maximum number of SMS challenges. | **Check for High Risk Score = TRUE**<br>Questions Active = Any<br>Challenge Email Available = Any<br>**Challenge SMS Available = TRUE**<br>Max failed Question Attempts = Any<br>Max failed Email Attempts =Any<br>**Max failed SMS Attempts = False** | Policy = NONE<br>Action = OAAM Challenge SMS<br>Alert = NONE<br>Score = 0 |
| Challenge the user with email if the risk score is High and he has registered for email and he did not fail the email challenge the maximum number of times yet. | **Check for High Risk Score = HIGH**<br>Questions Active = Any<br>**Challenge Email Available = TRUE**<br>Challenge SMS Available = Any<br>Max failed Question Attempts = Any<br>**Max failed Email Attempts = FALSE**<br>Max failed SMS Attempts = Any | Policy = NONE<br>Action = OAAM Challenge Email<br>Alert = NONE<br>Score = 0 |
| Challenge the user with questions if he has challenge questions active and has not failed the maximum number of challenges for questions | Check for High Risk Score = Any<br>**Questions Active = TRUE**<br>Challenge Email Available = Any<br>Challenge SMS Available = Any<br>**Max failed Question Attempts = TRUE**<br>Max failed Email Attempts = Any<br>Max failed SMS Attempts = Any | Policy = NONE<br>Action = OAAM Challenge Question<br>Alert = NONE<br>Score = 0 |
| Challenge the user with OTP via SMS if he has not failed Challenge SMS and he is registered for SMS. | Check for High Risk Score = Any<br>Questions Active = Any<br>Challenge Email Available = Any<br>**Challenge SMS Available = TRUE**<br>Max failed Question Attempts = Any<br>Max failed Email Attempts = Any<br>**Max failed SMS Attempts = FALSE** | Policy = NONE<br>Action = OAAM Challenge SMS<br>Alert = NONE<br>Score = 0 |

*Table 11–22   (Cont.) OAAM Challenge Trigger Combinations*

| Description | Combination Detail | Result |
|---|---|---|
| Challenge the user with email if he is registered for email and he did not fail the email challenge the maximum number of times yet. | Check for High Risk Score = Any<br>Questions Active = Any<br>**Challenge Email Available = TRUE**<br>Challenge SMS Available = Any<br>Max failed Question Attempts = Any<br>**Max failed Email Attempts = FALSE**<br>Max failed SMS Attempts = Any | Policy = NONE<br>Action = OAAM Challenge Email<br>Alert = NONE<br>Score = 0 |
| Block the user if he has not registered for questions or OTP and the risk score is High. This block can be overridden using the "Temp Allow" functionality. | **Check for High Risk Score = TRUE**<br>**Questions Active = FALSE**<br>**Challenge Email Available = FALSE**<br>**Challenge SMS Available = FALSE**<br>Max failed Question Attempts = Any<br>Max failed Email Attempts = Any<br>Max failed SMS Attempts = Any | Policy = NONE<br>Action = OAAM BLOCK<br>Alert = NONE<br>Score = 0 |
| Challenge Block the user if he failed to answer all types of challenge mechanisms. Note: This block cannot be overridden through the "Temp Allow" functionality. | All rules with result = ANY | Policy = NONE<br>Action = OAAM Challenge BLOCK<br>Alert = NONE<br>Score = 0 |

## 11.5.10  OAAM Customer Care Ask Question

This policy determines if the user has active questions, more questions left for the challenge, and how many challenges have failed.

### 11.5.10.1  OAAM Customer Care Ask Question Policy Summary

Table 11–23 provides a summary of the OAAM Customer Care Ask Questions Policy.

*Table 11–23   OAAM Customer Care Ask Question Policy*

| Summary | Details |
|---|---|
| Purpose | Determines if the user has active questions, more questions remaining for challenges, and how many challenges have failed. |
| Scoring Engine | Weighted Maximum |
| Weight | 100 |
| Group Linking | All Users |

### 11.5.10.2  OAAM Customer Care Ask Question: Details of Rules

Table 11–24 shows the rule conditions and parameters in the OAAM Customer Care Ask Questions Policy.

*Table 11–24    OAAM Customer Care Ask Question Rule Details*

| Rule | Rule Condition and Parameters | Results |
|---|---|---|
| No Questions | **USER: Question Status**<br><br>Triggers when users do not have questions registered. Two possible scenarios are un-registered users and users with questions reset by customer care.<br><br>Question status of the user<br><br>User Question Status=Not Set<br><br>Is=True | Action = OAAM No User Questions<br><br>Alert = NONE<br><br>Score = 0<br><br>Weight=100 |
| Maximum Answers Failed | **USER: Challenge Channel Failure**<br><br>Triggers when user failed maximum allowed answers with current question. Count is combination of customer care and online challenge.<br><br>If a user has a failure counter value over a specified value from specific channel<br><br>Challenge Channel=<select><br><br>Current Question Count only? = true<br><br>Failures greater than or equal to = 3 | Action = OAAM Next Question<br><br>Alert = NONE<br><br>Score = 0<br><br>Weight=100 |
| Question Blocked | **User: Challenge Question Failure**<br><br>Checks how many questions have failures<br><br>Failure more than or equal to=1 | Action = OAAM Reset Question<br><br>Alert = NONE<br><br>Score = 0<br><br>Weight=100 |
| Maximum Questions Failed | **User: Question Failure**<br><br>Triggers when user fails the maximum allowed questions.<br><br>Failure more than or equal to=3 | Action = NONE<br><br>Alert = NONE<br><br>Score = 0<br><br>Weight=100 |

### 11.5.10.3  OAAM Customer Care Ask Question: Trigger Combinations

None

# 11.6  Use Cases

The following sections provide security policy use case scenarios.

## 11.6.1  Use Case: WebZIP Browser

All users using a WebZIP browser must be blocked from attempting a login.

1. user1 uses WebZip and tries to log in to the application.

2. user1 is blocked.

3. The administrator logs in to OAAM Admin.

4. The administrator views the session for user1.

5. The administrator sees that **Rule: "WEBZIP" used** was triggered.

## 11.6.2 Use Case: IP Risky User OTP Challenge

User "test user" is a registered user. He is traveling on business to a different country and does not have access to email or phone. The IP he logs in from is considered a risky IP and hence, he is challenged by SMS. Since he cannot access his OTP, he fails to answer the OTP challenge by SMS. He is now challenged via KBA and unfortunately, he forgot the answers to his challenge questions. He guesses and answers the questions incorrectly. He is now locked out of the system. He calls the CSR and proves his identity. The CSR unlocks the user so he can log in again.

1. OTP is set up for SMS and Email.

2. The auto-learning policy (OAAM does user have profile) is disabled.

3. The user is registered as `testuser`.

4. His IP is in the Risky IP group.

5. `testuser` tries to log in to the application.

6. `testuser` is challenged via SMS.

7. `testuser` answers incorrectly 3 times.

8. `testuser` is challenged via KBA.

9. `testuser` answers challenge question incorrectly 3 times.

10. `testuser` is locked out.

11. CSR must create a case and then unlock challenge questions for the user.

12. `testuser` is able to log in to the application successfully.

## 11.6.3 Use Case: Anonymizer IP - From the Group

User "anonymizer" logs in using an IP which is considered an anonymizer in the Quova geolocation database. The user is blocked and a case is automatically created with the proper information. The investigator works on the case, adds a disposition, and closes the case.

**Administrator**

1. The administrator logs in to OAAM Admin.

2. He creates a new action instance using the action template "Create customer care case".

3. He selects the "post -authentication" checkpoint, the Block action, a score of "1000," and case type "2".

**User**

1. New user "anonymizer" tries to log in to the application.

2. The user is blocked.

   A fraud case is automatically created.

**Investigator**

1. The investigator logs in to OAAM Admin as an Investigator.

2. He opens the case and adds notes.

3. He closes the case with a disposition.

## 11.6.4 Use Case: Pattern Based Evaluation

User "test user2" is a registered user. He resides in the United States and hence, all his logins are typically from the United States. He is traveling on business to China and performs a few logins from there. Since OAAM identifies that this is not the normal behavior, it challenges the user.

Rules:

- The rule only triggers when the device used appears to have traveled faster than 600 MPH in the last 20 hours. A trigger results in a challenge action and appropriate and informative alerts sufficient enough to determine why the challenge was generated.

- The following rule only triggers a challenge action when both conditions are false: Has this user used this country more than 2 times ever?

  AND

  Has this user used this country more than 10% in the last month?

- If a user is challenged post-authentication, and he has KBA active, and he does not have OTP active and the risk is above 600, then he should be asked a KBA question.

# 12

# Managing Groups

Groups are like items that have been collected to simplify configuration workloads.

This chapter introduces you to the concept of groups and the different types of groups used in Oracle Adaptive Access Manager, and provides information on creating groups and editing group memberships, and group details. It also provides details on importing and exporting groups.

## 12.1 About Groups

As the security administrator, you must configure rules for actions and alerts, and rule conditions for users, locations and IPs, and so on.

For example, to create a rule "Restricted IPS," you must add a condition to find out if the user IP used for login is in the list of restricted IPs configured. The restricted IPs are grouped together as RestrictedIPSGroup of type IP and the rule condition uses this group.

## 12.2 Group Types

The following types of groups are available:

*Table 12–1   Group Types*

| Type | Description |
| --- | --- |
| ASN | This group holds ASNs. Autonomous System numbers (ASNs) are globally unique identifiers for Autonomous Systems. An Autonomous System (AS) is a group of IP networks having a single clearly defined routing policy, run by one or more network operators. |
| Actions | This group holds the different out-of-the-box actions. |
| | An action is an event activated when a rule is triggered. For example, block access, challenge question, ask for PIN or password, and so on. |
| | This is an enum group type. |
| Alerts | This group contains four kinds of alerts with four levels of severity. |
| | An alert is a message generated when a rule is triggered. For example, "login attempt from a new country for this user." |
| | Kinds of alerts are Fraud, Customer Care, Information, and Investigation. |
| | Alert levels are Low, Medium, High, and Info. |
| | Alerts are a special enum group type. |
| Authentication Status | This group contains the status of the user when logging in. |
| | This is an enum group type. |

*Table 12–1 (Cont.) Group Types*

| Type | Description |
| --- | --- |
| Cities | This group contains cities. For example, Presque Isle, Alakanuk, Chattahoochee, and so on. |
| Connection Speed | This group contains the internet connection speeds or bandwidths (high, medium, low). |
| | This is an enum group type. |
| Connection Type | This group contains connection types. Common connection types to the internet are Optical, T1/T3, Satellite, Cable, ISDN, Wireless, and so on. |
| | This is an enum group type. |
| Countries | This group contains countries. For example, black-listed countries. |
| Devices | This group contains devices IDs. Device IDs are unique identifications for devices such as PDA, cell phone, kiosk, and so on. For example, black-listed devices. |
| Generics | This group contains members related to string, integer, or long number information. |
| Generic Longs | This group contains long numbers. For example, stolen Social Security numbers, credit card numbers, or MAC addresses. |
| Generic Strings | This group contains generic strings. For example, if you wanted to permit anyone who has a variation of Smith to log in (Smithson, Smithberg, Smithstein, and so on), then you could define a prefix string of "Smith" for comparison. Another example: if you want to block anyone from Pennsylvania, Transylvania, Spotsylvania, and so on, from logging in, you can define a suffix string. |
| IP Carriers | This group contains carriers of Internet Protocol (IP) traffic. |
| IP Ranges | This group contains a range of IPs. |
| IPs | This group contains the IP addresses of the users. |
| | Addresses may map to locations, although some addresses are unknown or private (for example, 10.0.0.1). |
| ISP | This group contains Internet Service Providers. Examples of ISPs are Comcast, Verizon, AOL, and so on. |
| User Name | This group contains login names of users. It is set up by the user. For example: "Bob" is the login and the user is "xyz123." |
| | User name may not be unique across applications. The unique combination would be the Organization ID with the user name. |
| Routing Type | This group contains routing types. Examples of routing types are POP, Satellite, Anonymizer, International, and so on. |
| | This is an enum group type. |
| Second-level Domains | This group contains second-level domain names. |
| | A second-level domain is a domain directly below a top-level domain (TLD). Second-level domains commonly refer to the organization that registered the domain name. |
| | Second-level domain names can be used to pass and block whole sites such as *.example.org or entire intranet levels such as *.sales.* or *.admin.* |
| States | This group contains states. For example, black-listed states. |

*Table 12–1   (Cont.)  Group Types*

| Type | Description |
| --- | --- |
| Top-level Domains | This group contains top-level domain names (the last part of an Internet domain name, that is, the letters that follow the final dot of any domain name). |
| | Top-level domain names can be used to pass and block whole countries, for example,.uk, .ru, or .ca, and entire communities, for example, .mil, .info, .gov, or edu. |
| Transaction Status | This group contains the status of the user when a transaction is being performed. |
| | This is an enum group type. |
| User ID | This group contains User IDs. The customer uses a scheme to uniquely identify users. |
| | The User ID may not be unique across applications. The unique combination would be the Organization ID with the User ID. |
| | A special type of group is the Organization ID. Organization ID is a primary user group. A flag is set so that when users log in from the application, they are autopopulated into the group if they are not already members. You can use members of that group to scope policies. |

## 12.3  Group Usage

Groups are used in the following items:

- Policies

  A policy is linked to a User ID group or all users and members of the user group or all users that are evaluated.

  The Policy Tree shows the linking of User ID groups to policies.

- Rules within policies

  OAAM Admin applies rules on specified users, devices, or location groups to evaluate whether a fraud scenario occurred and to determine an outcome.

  A rule can trigger an action group, or an alert group, or both.

- Conditions

  Some conditions use groups as a parameter type. For example, IP in IP Group. The condition takes IP Group name / IP as a parameter.

- Trigger combinations

  Alerts in groups are specified in the trigger combination.

- Pre-condition

  User groups can be excluded in a policy.

- Configurable Actions

  Members of a User ID group can be added to a User ID group dynamically using configurable actions.

## 12.4  User Flows

In the create and edit user flow, you always begin by searching for a group and then viewing the details before deciding if you want to update group membership, edit group details, or edit group members, or if you want to define a group.

As an example user flow, the group creation flow, is shown in Figure 12–1.

*Figure 12–1   Group Creation Flow*
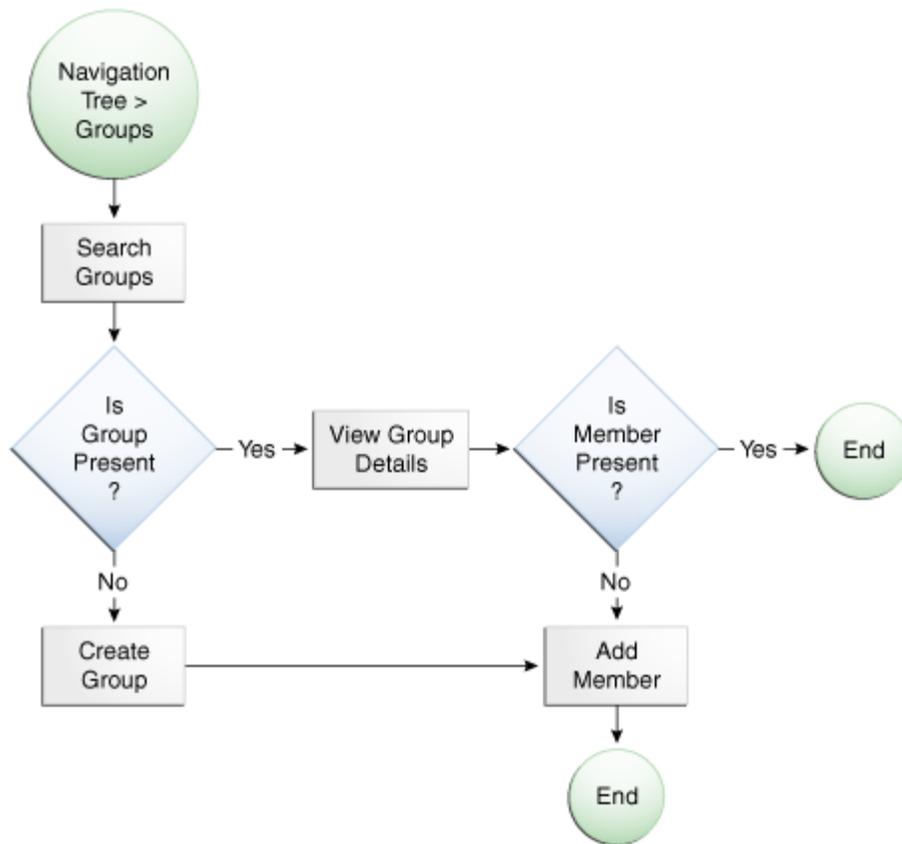


## 12.5  Navigating to the Groups Search Page

From the **Groups Search** page, you can search, view, create, import, export, and delete groups.

To open the **Groups Search** page:

1. Log in to OAAM Admin.

2. From the Navigation tree, select **Groups**. The **Groups Search** page is displayed.

   Alternative methods to open search pages are listed in Section 3.9, "Search, Create, and Import."

   The **Groups Search** page displays a Search section and a **Search Results** table that shows a summary of the groups that match your search criteria.

*Figure 12–2   Groups Search page*



## 12.6  Searching for a Group

When the **Groups Search** page first appears, the **Search Results** table is empty. You must press **Search** to see a list of groups in the Oracle Adaptive Access Manager environment.

In the **Groups Search** page, you can search for a specific group you are interested in by using the specific criteria in the search filter.

To search for a group:

1. Navigate to the **Groups Search** page, as described in Section 12.5, "Navigating to the Groups Search Page."

2. Specify criteria to locate the group and click **Search**.

   Clicking **Reset** instead of **Search** resets the search criteria.

   Search parameter values are not required. If you choose to leave the fields blank, all groups are displayed in your search results.

The search filters are described in Table 12–2.

**Table 12–2    Groups Search Filter Criteria**

| Filters and Fields | Descriptions |
| --- | --- |
| Group Name | Name of the group. You can enter the complete name or part of a group name. For example, if you enter new, any group with new in any part of its name is displayed. |
| Cache Policy | Groups offer two Cache 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 and read-only groups are good candidates for the "Full Cache" option. Administrators must 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" Cache Policy option does not use cache and consults the database every time. Device group types are set to "None" because in most cases, they are dynamic and manipulated while the server is running. If you have groups that stay static for the lifetime of the server, you can use the "Full Cache" option instead of "None." |
| Group Type | Category to which the group belongs. The types are listed in Table 12–1 |

The groups that are displayed are those that match the criteria specified in the **Group Name**, **Group Type,** and **Cache Policy** fields.

The option to sort is provided on every column in the **Search Results** table.

Each group has a name. If the description is too long to be fully shown, you can place the mouse over the text to see the entire description.

In the **Search Results** table, click the hyperlinked group name of the group you are interested in to view more details.

## 12.7  Viewing Details about a Group

The **Group Details** tab has summary, member, and usage tabs.

To view details about a group:

1. Navigate to the **Groups Search** page, as described in Section 12.5, "Navigating to the Groups Search Page."

2. Enter the name of the group in the **Group Name** field and click **Search**.

3. Click the group name to view the **Group Details** page for that group.

   The **Summary** tab shows general information about the group, such as the name, type, cache policy, and description of the group.

   > **Note:**  You cannot change the group type in the **Group Details** page.

4. From the members tab, you can add members to the group or select members of the group to remove.

   The members tab is labeled with the data type the group contains. For example, a User ID group has a member tab labeled **User ID**.

   The members tab shows all the members of the group. The members tab typically shows member name/ ID, description, and any other critical attributes of members. The exact information differs depending on the group type.

> **Note:** ·You cannot edit existing **Action** elements and their properties.

5. From the Usage tab, you can view all the different locations a group is used (conditions, overrides, configurable actions and so on) in a hierarchical fashion. If the group is not used, you are not able to access the tab.

   You can view the details of any node in the usage tree. For example, when you click Rule A above Precondition xyz, the right hand side panel shows brief details about Rule A and you can view additional details, if needed.

6. To view details about the entity that the group is used in, click its link.

   Clicking the link launches the details page of that particular item in a new tab.

## 12.8  Adding an Entity to a Group

You could add an entity to a group or create a group and add the entity to it, or remove an entity from a group, using the Add to Group button from details pages.

The Add to Group feature is described below:

*Table 12–3    Add to Group*

| Feature | Description |
| --- | --- |
| Add entity to entity group | You can select an entity group from a list of entity groups with which the entity is not already associated and add the entity to it. A User Group can be either a User ID or User Name group type. |
| | An entity cannot be added to the same entity group multiple times with the exception of the alert. |
| | An alert can be added to an Alert Group multiple times, since whenever an alert is added to an Alert Group, a new instance of the existing alert is created and added to the group. |
| Create a new entity group and add entity to the newly created group. | You can create a new entity group and add the entity to it. A user group can be of either User ID or User Name group type. |
| Remove entity from entity group | You can select multiple entity groups with which it is already associated and remove the entity from the selected groups. Note: Removing users from Organization ID is not recommended. |

## 12.9  Group Characteristics

The following table shows a summary of group characteristics.

The **Group** column shows the type of groups available in the system.

The **Group Member Type** column shows whether the record is a primitive type (long, string, and integer) or a structured type. An example of a structured type is Actions, which has name, ID, and message

The **Cache** column shows the cache option that is recommended for the group.

The **Create** column shows whether the group can be created using the user interface for groups.

The **Edit** column shows whether the group can be edited using the user interface for groups.

*Table 12–4    Summary of Group Characteristics*

| # | Group | Group Member Type | Cache | Create | Edit |
|---|-------|-------------------|-------|--------|------|
| 1 | Actions | Struct | Yes | No | No |
| 2 | Authentication Status | Long | Yes | No | No |
| 3 | Connection type | Long | Yes | No | No |
| 4 | Connection speed | Long | Yes | No | No |
| 5 | Routing Type | String | Yes | No | No |
| 6 | Transaction Status | Struct | Yes | No | No |
| 7 | Alerts | Struct | Yes | Yes | Yes |
| 8 | Generic Integers, Generic Strings, Generic Long | Integer, String, Long | Yes | Yes | Yes |
| 9 | ASN | String | Yes | Yes | Yes |
| 10 | IP Carriers | String | Yes | Yes | Yes |
| 11 | Top-level Domains | String | Yes | Yes | Yes |
| 16 | Second-level Domains | String | Yes | Yes | Yes |
| 12 | Cities | String | Yes | No | No |
| 13 | Countries | String | Yes | No | No |
| 14 | States | String | Yes | No | No |
| 15 | ISPs | String | No | Yes | Yes |
| 17 | Device ID | Long | Yes | Yes | Yes |
| 18 | IPs | IP | Yes | Yes | Yes |
| 19 | IP Ranges | Struct | Yes | Yes | Yes |
| 20 | User Name | String | Yes | Yes | Yes |
| 21 | UserId groups | String | Yes | Yes | Yes |

## 12.10  Creating a Group

The process for creating a group involves:

1. Defining a Group

2. Adding Members to a Group

### 12.10.1  Defining a Group

The same group name cannot exist across the group types. For example, if an action group called "Block" exists, you cannot create user name group called "block".

The steps for defining a group are:

Group Name and Group Type are required fields.

1. In the Navigation tree, double-click **Groups**. The **Groups Search** page is displayed.

2. From the **Groups Search** page, click the **New Group** button or icon.

Alternative methods to open create pages are listed in Section 3.9, "Search, Create, and Import."

The **Create Group** screen is displayed.

3. In the **Create Group** screen, enter a group name and description.

   The group name must be unique.

4. From the **Group Type** list, select a group type.

   The types are listed in Table 12–1

*Figure 12–3   Create Group screen*



5. Set the cache policy to **Full Cache** or **None**.

   > **Note:** ISP groups cannot be cached.

6. Click **OK** to create the group or **Cancel** to disregard the changes.

   If you click **OK**, a new group is created.

   A confirmation dialog is displayed.

7. Click **OK** to dismiss the dialog.

   The **Group Details** page for the new group is displayed.

   Now, you can add members to the new group.

## 12.10.2  Adding Members to a Group

You can add members to a new or an existing group.

Because there are multiple group types, the procedure you perform to add members to a group depends on the group type. Refer to the following tables for the appropriate procedure for the group you are creating.

> **Note:** When group members are added to certain group types like "blacklisted countries," they are processed automatically since the rules are pre- configured.
>
> For example, the rule "Check if login is from a blacklisted country" is pre-configured and attached to "blacklisted countries" by default. Hence adding members to this group automatically starts rules processing.

When you search for members, the ones that are already part of your group are not available in your search results.

> **Note:** The server must be restarted for enum elements to take effect. Enum group types are actions, connection speed, connection type, and so on.

### Create a new member to add to the group (no search/ filter option)

Table 12–5 lists groups that add members without an option to search or filter.

If you are adding members to a group listed in Table 12–5, see Section 12.11, "Creating a New Element/Member to Add to the Group (No Search and Filter Options)."

*Table 12–5    Create New Member (No Search Option)*

| Group | Group Type | Member Type | Create |
|---|---|---|---|
| Generic Integers, Generic Strings, Generic Long | Database | Integer, String, Long | Yes |
| ASN | Database | String | Yes |
| IP Carriers | Database | String | Yes |
| Top-level Domains | Database | String | Yes |
| Second-level Domains | Database | String | Yes |

### Add members from cities, states, and countries by filtering an existing list (no creation option)

Table 12–6 lists groups that add members from cities, states, or countries by filtering an existing list to find members and then adding the members to the group. The element cannot be created for these groups.

If you are adding members to a group listed in Table 12–6, see Section 12.12, "Filtering an Existing List to Select an Element to Add to the Group (No Creation of a New Element)."

*Table 12–6    Add Members by Filtering Existing (No Creation Option)*

| Group | Group Type | Member Type | Create |
|---|---|---|---|
| Cities | Database | String | No |
| Countries | Database | String | No |
| States | Database | String | No |

### Search for existing elements or create new elements

Table 12–7 lists groups that add elements by searching existing elements or creating new elements and then adding them to the group.

If you are adding elements to a group listed in Table 12–7, see Section 12.13, "Searching for and Adding Existing Elements or Creating and Adding a New Element."

*Table 12–7    Search for existing or create new elements*

| Group | Group Type | Member Type | Create |
|-------|-----------|-------------|--------|
| ISPs | Database | String | Yes |
| Device ID | Database | Long | Yes |
| IPs | Database | IP | Yes |
| IP Ranges | Database | Struct | Yes |
| User Name | Database | String | Yes |
| UserId groups | Database | String | Yes |

### Adding Alerts

For alerts you have the option to either search for an existing alert or create a new alert before adding it to the Alert group.

If you are adding alerts to an Alert group, see Section 12.14, "Adding Alerts to a Group."

### Search and add existing elements only (No Creation)

Table 12–8 lists the groups that add members by searching for existing elements and then adding them to the group. You do not have the option to create a new element through the Groups user interface. To create a new element, you must use the Properties Editor.

If you are adding elements to a group listed in Table 12–8, see Section 12.15, "Searching for and Adding Existing Elements."

*Table 12–8    Search and add existing only (no creation option)*

| Group | Group Type | Member Type | Create |
|-------|-----------|-------------|--------|
| Actions | Enum | Struct | No |
| Authentication Status | Enum | Long | No |
| Connection type | Enum | Long | No |
| Connection speed | Enum | Long | No |
| Routing Type | Enum | String | No |
| Transaction Status | Enum | Struct | No |

## 12.11  Creating a New Element/Member to Add to the Group (No Search and Filter Options)

The following groups add new elements/members by entering values for the elements.

- ASN
- Generic Integers
- Generic Longs
- Generic Strings

- IP Carriers

- Second-level Domains

- Top-level Domains

To add an element to a group:

1. In the **Group Details** page, click **Add Member**.

   The **Add Member** dialog is displayed.

2. In the **Add Member** dialog, enter the value for the new member that are added to the group.

*Table 12–9    Create Parameters*

| Group | Create Parameters |
| --- | --- |
| Generic Integers, Generic Strings, Generic Long | Value |
| ASN | ASN |
| IP Carriers | Name |
| Top-level Domains | Name |
| Second-level Domains | Name |

3. Click **Add** to add the member to the group or **Cancel** to disregard the changes.

   If you click **Add**, the member is created and added. A confirmation is displayed with the message, "The new element created successfully."

4. Click **OK**.

   The **Group Details** page is displayed.

## 12.12  Filtering an Existing List to Select an Element to Add to the Group (No Creation of a New Element)

The following groups listed add members by filtering an existing list and then selecting an element to add. The element cannot be created for these groups.

- Cities

- States

- Countries

---

> **Note:**    To create a city, state, or country location group, you must populate the geolocation data. Geolocation data provides information about countries, states, and cities.

---

### 12.12.1  Adding a City to a Cities Group

To add cities to a cities group:

1. In the Cities tab of the **Group Details** page, click **Add**.

   The **Add Cities** dialog is displayed.

2. Select the country from the available country drop-down.

   The states of that country are made available in the states drop-down.

3. Select the state from the available states drop-down.

   Based on the selection of the state, the cities are listed in the **Available Cities** table.

4. From the **Available Cities** table, select one or more cities to add to the group.

5. Click **Add**.

   The cities are added successfully to the group.

### 12.12.2  Adding a State to a States Group

To add states to a states group:

1. In the **States** tab of the **Group Details** page, click **Add**.

   The **Add Member** dialog is displayed.

2. Select a country.

   On selection of the available country, the available states are listed in the **States** table.

3. From the **Available States** table, select one or more states to add to the group.

4. Click **Add**.

   The states are added successfully to the group.

### 12.12.3  Adding a Country to a Country Group

To add countries to a countries group:

1. In the **Countries** tab of the **Group Details** page, click **Add**.

   The **Add Member** dialog is displayed.

2. From the **Available Countries** table, select one or more countries to add to the group.

3. Click **Add**.

   The countries are added successfully to the group.

## 12.13  Searching for and Adding Existing Elements or Creating and Adding a New Element

For the following groups listed you have the option to either search for and add existing elements or create a new element to add.

- IP Range
- User ID
- Devices
- User Name
- IP
- Internet Service Provider

When you search for members, the ones that are already part of your group are not available in your search results.

Because the procedures for alert groups are different from the other groups listed earlier, separate sections are provided.

## 12.13.1  Selecting an Element to Add as a Member to the Group

To add an existing element as a member of the group, follow these steps:

1.  In the **Group Details** page, click **Add Member**.

    The **Add Member** page is displayed.

2.  In the **Add Member** page, select **Search and select from the existing elements**.

*Figure 12–4   Search and Select Member*



3.  Specify the filter criteria to find an element or list of elements and click **Search**.

*Table 12–10   Searching for Elements*

| Search Filter | Description |
| --- | --- |
| Application ID | An application identifier used to look up properties based on application. |
| User ID | User's identification number |
| User Name | Login name of the users |

**Table 12–10   (Cont.)  Searching for Elements**

| Search Filter | Description |
|---|---|
| Device ID | String that uniquely identifies each device and is autogenerated by the application |
| IP Address | Address mapped to a location usually, although some addresses are unknown or private |
| Group Name | Name of the group. You can enter the complete name or part of a group name. For example, if you enter new, any group with new in any part of its name is displayed. |

4. Select each element you want to include in the group.

5. Click **Add** to add the element as a member of the group or **Cancel** to disregard the changes.

   If the element is added successfully, a confirmation is displayed.

6. Click **OK** to dismiss the dialog.

**Example 1: Adding a Device to a Group of Interest Using Groups Interface**

To add an existing device to a group:

1. Log in to the OAAM Admin Console.

2. Double-click **Groups** in the Navigation tree.

3. Search for the Device group.

4. In the Search Results table, click the name of the Device group. The Device Details page appears.

5. Click **Members** tab.

6. Click the **Add Member to this Group** icon on the toolbar. The **Add Devices** dialog appears.

7. Choose the **Search and select from the existing Devices** option and search for the Device ID.

8. Select the Device ID and click **Add**.

9. Click **OK** to dismiss the confirmation dialog.

**Example 2: Adding an IP to a Group of Interest Using the Groups Interface**

To add an existing IP to a group:

1. Log in to the OAAM Admin Console.

2. Double-click **Groups** in the Navigation tree.

3. Search for the Device group.

4. In the Search Results table, click the name of the Device group. The Device Details page appears.

5. Click **IPs** tab.

6. Click the **Add Member to this Group** icon on the toolbar. The **Add Devices** dialog appears.

7. Choose the **Search and select from the existing IPs** option and search for the IP address.

8. Select the IP address and click **Add**.

9. Click **OK** to dismiss the confirmation dialog.

## 12.13.2 Creating an Element (Member) to Add to the Group

To create a new member and add it to the group:

1. In the member tab of the **Group Details** page, click **Add Member**.

2. In the **Add Member** page, select **Create New Element**.

*Figure 12–5   Add Member*



3. Type in the values for the member.

*Table 12–11   Create Parameters*

| Group | Create Parameters |
| --- | --- |
| ISPs | NA |
| Device ID | Device ID |
| IPs | IP |
| IP Ranges | From IP |
| | To IP |
| | Description |
| Login Ids | Login ID |
| UserId groups | User ID |

4. Click **Add** to create and add the new member to the group or **Cancel** to disregard the changes.

If the new element was created successfully, a confirmation dialog is displayed.

5. Click **OK** to dismiss the dialog.

## 12.14 Adding Alerts to a Group

Procedures for adding alerts to an alert group are provided in the following sections.

## 12.14.1 Selecting an Existing Alert to Add to the Alert Group

To select from existing alerts to add to an alert group:

1. In the **Alerts** tab of the **Group Details** page, click **Add Member**.

2. In the **Add Member** page, select **Search and select from the existing elements**.

3. Specify the criteria for the specific alert or a list of alerts you are interested in and click **Search**.

*Table 12–12    Searching for Alerts*

| Search Criteria | Description |
| --- | --- |
| Alert Message | Message to notify administrators |
| Level | High, Information, Low, Medium |
| Type | CSR, Fraud, Information, Investigation |

4. In the **Search Results** table, select the alerts you want to include in the alert group.

5. Click **Add** to add the alerts to the group or **Cancel** to disregard the changes.

    If you click **Add**, the alerts are added.

    A confirmation dialog is displayed.

6. Click **OK** to dismiss the dialog.

    The **Group Details** page is displayed with the added alerts.

When an existing alert is added to another group, a copy of the alert is added with a different unique Alert ID. If you were to change the message in one of the alerts, the change does not propagate to the other alerts.

## 12.14.2  Creating a New Alert to Add to the Alert Group

To create a new alert to add to the alert group:

1. In the **Alerts** tab of the **Group Details** page, click **Add Member**.

2. In the **Add Member** page, select **Create new element**.

*Table 12–13    Create Parameters for Alerts*

| Group | Create Parameters |
| --- | --- |
| Alerts | Alert Type |
|  | Alert Level |
|  | Alert Message |

3. Select the alert type.

    The alert types you can select from are **Fraud**, **Customer Care**, **Information**, **Investigation**.

4. Select the alert level.

    The alert levels to select from are **Low**, **Medium**, **High**, and **Information**.

5. Type in the alert message in the **Alert Message** box.

    For example: a "High Fraud" alert may require that you notify a manager (and the customized message has the manager's phone number), whereas an "Info" Information alert may have no message at all.

*Figure 12–6  Create an alert*



6. Click **Add** to create and add the new alert to the alert group or **Cancel** to disregard the changes.

   If you click **Add**, the alert is added.

7. When the confirmation dialog appears, click **OK** to dismiss the dialog.

## 12.15  Searching for and Adding Existing Elements

For the following groups listed you can only search and add existing elements to the group. You do not have the option to create a new element.

- Authentication Status

- Connection Type

- Connection Speed

- Routing Type

- Transaction Status

- Actions

To create or edit elements, you must use the Properties Editor.

When you search for members, the ones that are already part of your group are not available in your search results.

Because the procedure for the action group is different from the other groups listed earlier, a separate section is provided for actions.

### 12.15.1  Selecting an Element to Add as a Member to the Group

To add an existing element as a member of the group, follow these steps:

1.  In the **Group Details** page, click **Add Member**.

    The **Add Member** page is displayed.

2.  In the **Add Member** page, select **Search and select from the existing elements**.

3.  Specify the filter criteria to find an element or list of elements and click **Search**.

4.  Select each element you want to include in the group.

5.  Click **Add** to add the element as a member of the group or **Cancel** to disregard the changes.

    If the element is added successfully, a confirmation is displayed.

6.  Click **OK** to dismiss the dialog.

## 12.15.2  Adding Actions to an Action Group

Follow these steps for adding actions to an action group:

### 12.15.2.1  Selecting an Existing Action to Add to an Action Group

To search and select an action from existing actions:

1.  In the **Actions** tab of the **Group Details** page, click **Add Member**.

2.  In the **Add Member** page, select **Search and select from the existing elements**.

3.  Search for a specific action or a list of actions by using the Search filter and clicking **Search**.

    The list of actions includes actions, such as **Allow**, **Block**, **Challenge**, and others.

*Figure 12–7 Search for an Action*



4. Select the row for each action you want to include in the group and click **Add**.

5. When the confirmation dialog is displayed, click **OK**.

   The actions are added to the **Action Group** and the **Group Details** page displays the new action.

### 12.15.2.2 Creating a New Action to Add to an Action Group

You can only search and add existing actions to the Action group. To create or edit actions, you must use the Properties Editor.

The actions that you create are only intended to be used as trigger actions for configurable actions. These actions do not have any effect on applications directly.

## 12.16 Editing a Member of a Group

To edit a member of a group, follow these steps:

For a list of the groups in which members can be edited, see Table 12–14, " Editing a Member of a Group".

1. Navigate to the **Groups Search** page, as described in Section 12.5, "Navigating to the Groups Search Page."

2. Specify criteria in the Search filter to locate the group that contains the member you want to edit.

3. Click **Search**.

4. In the list of groups, click the name of the group that contains the member.

5. In the **Members** tab, select the member and click the **Edit** button.

6. In the **Edit Element** screen, make the appropriate modifications.

7. Click **Apply** to save the changes or **Revert** to discard them.

*Table 12–14    Editing a Member of a Group*

| Group | Edit |
| --- | --- |
| Actions | No |
| Authentication Status | No |
| Connection type | No |
| Connection speed | No |
| Routing Type | No |
| Transaction Status | No |
| Alerts | Yes |
| Generic Integers, Generic Strings, Generic Long | Yes |
| ASN | Yes |
| IP Carriers | Yes |
| Top-level Domains | Yes |
| Second-level Domains | Yes |
| Cities | No |
| Countries | No |
| States | No |
| ISPs | Yes |
| Device ID | Yes |
| IPs | Yes |
| IP Ranges | Yes |
| Login Ids | Yes |
| UserId groups | Yes |

## 12.17  Removing Members of a Group

To remove members of a group:

1. Navigate to the **Groups Search** page, as described in Section 12.5, "Navigating to the Groups Search Page."

2. Specify criteria in the Search filter to locate the group with the members you want to delete.

3. Click **Search**.

4. In the **Results** table, select the group you want to remove members from.

   The **Group Details** page is displayed.

5. In the **Members** tab, select members of the group you want to remove and click **Delete**.

   A confirmation appears, asking if you want to delete the member from the group.

6. Click **Yes**.

   A dialog appears with the message that the selected member is deleted successfully.

7. Click **OK** to dismiss the dialog.

## 12.18 Removing a User from a User Group

To remove a user from a user group:

1. Navigate to the **Groups Search** page, as described in Section 12.5, "Navigating to the Groups Search Page."

2. Specify criteria to locate the group you want to remove the user from.

3. Click **Search**.

4. In the **Results** table, click the name of the user group.

5. In the **Group Details** page, click the **User ID** tab.

6. Select the row with the user ID of the user you want to remove and click **Delete**.

   A dialog appears with the message, "Are you sure you want to delete the member from the group?"

7. Click **Yes** to confirm.

   A confirmation dialog appears with the message, "Selected members are deleted successfully."

8. Click **OK** to dismiss the dialog.

## 12.19 Exporting and Importing a Group

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

### 12.19.1 Exporting a Group

To export a group:

1. Navigate to the **Groups Search** page, as described in Section 12.5, "Navigating to the Groups Search Page."

2. Specify criteria in the Search filter to locate the group.

3. Select all the rows corresponding to the groups you want to export.

4. Select **Export Selected** from the **Actions** menu.

5. When the export dialog appears, select **Save File**, and then **OK**.

   The file is exported and saved as a ZIP file.

## 12.19.2 Importing a Group

To import a group:

1. Navigate to the **Groups Search** page, as described in Section 12.5, "Navigating to the Groups Search Page."

2. In the **Groups Search** page, click the **Import Group** button. The **Import Groups** screen appears.

3. In the **Import Groups** dialog box, type the path and name of the file; or use the **Browse** (...) button to locate the ZIP file that contains the groups, and then select the file.

4. Click **Open** and then click **OK**.

   An **Imported List** dialog appears with the list of groups that have been imported along with the general details.

5. Click **OK**.

   If the file contains groups with the same names as the existing groups, the groups are updated/overwritten. If the file contains groups with names that do not exist, the groups are added to the system.

   If you are importing a delete script, the groups are deleted from the system.

   If you try to import groups in an invalid format, an error is displayed.

## 12.20 Deleting Groups

To delete groups:

1. Navigate to the **Groups Search** page, as described in Section 12.5, "Navigating to the Groups Search Page."

2. In the **Groups Search** page, search for a specific group or a list of groups you are interested in by using the specific criteria in the Search filter and clicking **Search**.

3. Select the rows corresponding to each group you want to delete and click **Delete**.

   If the groups selected for deletion are not used or linked to a policy, a confirmation dialog is shown asking for a confirmation. If you answer "yes," those groups are deleted.

   When multiple groups are selected for deletion and if some of the groups are used or linked to other systems, a message appears, telling you which ones can be deleted and which ones are in use or linked and cannot be deleted. Links to a usage tree are available for each of the used/linked groups. In the dialog, you are also given the option to delete the ones that are not in use.

   A confirmation is displayed, asking if you are sure you want to delete the group.

4. Click **Yes** to delete the groups.

   A dialog is displayed with the message that selected groups are deleted successfully.

5. Click **OK** to dismiss the dialog.

## 12.21 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.

   For information, see Section 12.19.1, "Exporting a Group."

2. Open the XML and make the edits you want.

3. Import the group to either overwrite or append to the previous version.

   For information, see Section 12.19.2, "Importing a Group."

## 12.22 Use Cases

This section describes example use cases for groups.

### 12.22.1 Use Case: Migration of Groups

Chuck is an Administrator migrating a 10.1.4.5 deployment to 11*g* R1+. He must import his existing groups into the upgraded environment. All group types must be tested for proper migration between 10.1.4.5 and 11*g* R1+.

1. Open **Group** in the Navigation tree.

2. Click **Import Group** in **Groups Search** page.

3. Import ZIP file of exported groups.

   a. Browse for ZIP file containing groups.

   b. Click **OK**.

4. Import Groups confirmation screen appears with information about the groups imported (Group Name, Group Type, Cache Type, and Notes). Click **OK**.

### 12.22.2 Use Case: Create Alert Group and Add Members

The velocity rule you created (in Section 10.34.4, "Use Case: Add New Rule") needs an alert group assigned to it so investigators can easily see that a rule was triggered and why. Directions: Create a new alert group named "High velocity user." Craft a message about the velocity rule that would be useful to an investigator such as this "User appears to have traveled faster than 500 MPH since last login."

To create an alert group and add members:

1. Log in to OAAM Admin as a security administrator.

2. In the Navigation tree, double-click **Groups**. The **Groups Search** page is displayed.

3. In the **Groups Search** page, search for an existing alert group you can reuse.

   a. Search for a group with **Alerts** as the **Group Type** and "velocity" as part of the **Group Name**.

   b. Select the group from the **Search Results** table.

   c. From the **Group Details** page, click the **Alerts** tab.

Alerts in the alerts group appear.

    **d.** Check to see whether any alerts suit your needs.

    **e.** Repeat Steps b, c, and d.

The alert groups do not contain the message that applies to your use case, so you decide to create a new one.

**4.** Create an **Alerts** group.

    **a.** Click the **New Group** to create a new alert group. The **New Group** screen is displayed.

    **b.** In the **Group Name** field, enter **High velocity user**.

    **c.** From the **Group Type** list, select **Alerts**.

    **d.** From the **Cache Policy** list, select the cache policy as "Full Cache."

    **e.** Enter a description in the **Description** field.

    **f.** Click **OK**. A confirmation message appears.

    **g.** Click **OK** to dismiss the confirmation dialog.

The new High velocity user group is created successfully and the Group Details page is displayed.

**5.** Add an alert with messaging about a user with non-plausible velocity.

    **a.** Click the **Alerts** tab to add alerts to the group.

    **b.** In the **Alerts** tab, click the **Add Member** button.

    **c.** In the **Add Member** page, select **Create new element**.

    **d.** For **Alert Type**, select **CSR**.

    **e.** For **Alert Level**, select **Medium**.

    **f.** For **Alert Message**, enter "User appears to have traveled faster than 500 MPH since last login."

    **g.** Click **Add** to add the alert to the group.

A confirmation dialog appears with the message, "The new element created successfully."

    **h.** Click **OK** to dismiss the dialog.

The High velocity user group appears in the **Search Results** table of the Groups Search page.

An alternative scenario for this adding the alert is to search for the message, "User appears to have traveled faster than 500 MPH since last login" and add that to the group.

## 12.22.3 Use Case: Remove User from Group

The restricted users group is intended for users who have had high risk activity. This practice helps protect the company and the users. The security team reviews the users in this group on a quarterly basis or when a customer issue is being looked at. Directions: Part A: Do a session search filtered to show only Phillip's activity for the last six months. Add Phillip to the restricted users group. Part B: Oops you made a mistake, please remove Phillip from the restricted users group since security team practices recommend this.

1. Log in to OAAM Admin as an investigator.

2. In the Navigation tree, double-click **Sessions**. The **Sessions Search** page is displayed.

3. In the **Sessions Search** page, perform a search using the following criteria.

   a. In the **Login Time** fields, enter start and end dates for the last six months.

   b. In **User Name** field, enter Phillip's user name.

   c. In the **Alert Level**, select **High**.

   There are no other high severity security alerts.

4. Copy Phillip's User ID from the search result's **User ID** column.

5. In the Navigation tree, double-click **Groups**.

6. In the **Groups Search** page, search for the **Restricted User** group.

7. In the **Results** table, click the group name, **Restricted User**.

8. In the **Group Details** page, click the **User ID** tab.

9. Click **Add**.

10. In the **Add Member** screen, select **Create new element**.

11. For **User ID**, enter Phillip's User ID and click **Add**.

    A confirmation dialog appears with the message, "The new element created successfully."

12. Click **OK** to dismiss the dialog.

    You learn that you made a mistake and must remove Phillip from the restricted users group since security team recommended this.

13. In the Navigation tree, double-click **Groups**.

14. In the **Groups Search** page, search for the **Restricted User** group.

15. In the **Results** table, click the group name, **Restricted User**.

16. In the **Group Details** page, click the **User ID** tab.

17. Select the row with Phillip's User ID and click **Delete**.

    A dialog appears with the message, "Are you sure you want to delete the member from the group?"

18. Click **Yes** to confirm.

    A confirmation dialog appears with the message, "Selected members are deleted successfully."

19. Click **OK** to dismiss the dialog.

### 12.22.4 Use Case: Block Users from a Black-listed Country

To block a user if the IP is in a given country group:

1. Navigate to the **Policies Search** page.

2. Enter the search criteria you want and click **Search**.

3. In the **Results** table, click the name of the policy you want to edit.

   The **Policy Details** page appears.

4. In the **Policy Details** page, click the **Rules** tab.

5. In the **Rules** tab, click **Add**.

6. In the **New Rule** page, enter the rule name as **Location: From IP**.

7. Click the **Conditions** tab.

8. In the **Conditions** page, click **Add**.

   The **Add Conditions** page is displayed where you can search for and select the **Location: In Country Group** condition and add it to the rule.

9. Click **OK**.

   The parameters for the condition are displayed in the bottom subpanel.

10. In the parameters area, for **Country in country group**, select the **Blacklisted Country** group.

11. Click **Save**.

12. In the **Results** tab, select **Block** as the action group.

13. Click **Apply**.

*Figure 12–8   Black-Listed Countries*
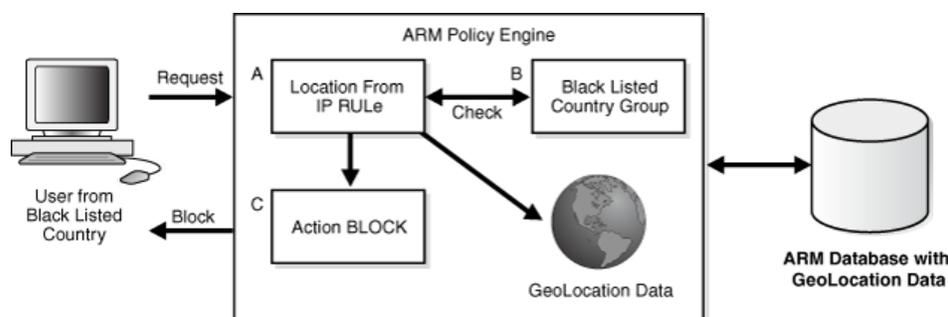


## 12.22.5  Use Case: Company Wants to Block Users

An example of how groups work in policies and rules is described in this section.

In this example, Company A observes a significant increase in high-risk alerts from a collection of countries where customers do not normally log in from. Company A wants to block users in those countries.

The steps to create a policy that blocks user of high-risk countries are summarized in the following subsections. Three groups are created for this policy.

### 12.22.5.1  Create Country Blacklist Policy (1): Create Fraudulent Country Policy and Rule

You must first create a Fraudulent Country policy with the following attributes:

*Table 12–15    Fraudulent Country Policy*

| Attribute | Value |
|---|---|
| Name | BlackListCountry |
| Checkpoint | Post-Authentication (executed after the user enters the password) |
| Status | Active |
| Scoring Engine | Maximum |
| Weights | 100 |
| Rule and Condition | Rule contains "Condition: Location: In Country group - True" |

### 12.22.5.2  Create Country Blacklist Policy (2): Create Country Group

A group type, "countries" contains the names of countries that have committed fraud.

Next, create a country group with the following attributes and then edit the group to add members.

*Table 12–16    Country Group*

| Attribute | Value |
|---|---|
| Group Name | Country_Blacklist |
| Group Type | Countries |
| Cache Policy | Full Cache |
| Description | OAAM Country Blacklist Group |

### 12.22.5.3  Create Country Blacklist Policy (3): Create Fraud High Alert Group

Alerts are indicators to fraud analysts. This alert group is used when a user from a blocked country logs in, the rule triggers and outputs a high alert. The group contains the alerts to trigger.

Create a Fraud High Alert group with the following attributes:

*Table 12–17    Fraud High Alert Group*

| Attribute | Value |
|---|---|
| Group Name | Loc_Blacklist |
| Group Type | Alerts |
| Cache Policy | Full Cache |
| Description | OAAM Location Blacklist Group |

Then, edit the group by setting:

- Alert Level to ALERT_HIGH
- Alert Type to Fraud
- Alert Message to LOC_BLACK LIST COUNTRY

### 12.22.5.4  Create Country Blacklist Security Policy (4 of 5): Create Block Action Group

The result of a rule is an action that is executed as what should take place if the user logs in from blocked country and in this case you block him indicating the client

application to redirect the user to a page with an appropriate message, "You Have Been Blocked."

Create a Block Action group with the following attributes:

**Table 12–18    Block Group**

| Attribute | Value |
| --- | --- |
| Group Name | Block |
| Group Type | Actions |
| Cache Policy | Full Cache |
| Description | Blacklist Action Group |

Edit group by selecting Block from Available Actions.

### 12.22.5.5  Create Country Blacklist Security Policy (5 of 5): Attach Groups to Fraudulent Country Rule

Attach the Blacklisted country group to the rule so that when the rule triggers all users logging in from the countries in this list are blocked.

1.  In OAAM Admin, query for **BlackListCountry** policy.

2.  Add **LocCountry_Rule** that has **Location: In Country group** condition.

3.  Define policy so that:

    ■   Is in group: **True**

    ■   Country in Country Group: **Country_blacklist**

    ■   Score: **1000**

    ■   Weight: **100**

    ■   Action Group: **Block**

    ■   Alert Group: **Loc_Blacklist**

4.  **Group Link** - Set Group type to **User ID**

5.  From **Group** select a group.

## 12.22.6  Use Case: Block Users from Certain Countries

If the policy is to block users from countries that have been identified for suspicious activities, you could create Block Country, Fraud High Alert, and Block Action groups.

■   **Block Country group** - Country names are populated in a group type "countries" that have been identified for fraud

■   **Fraud High Alert group** - This group contains the alerts to trigger to indicate to analysts that a fraud scenario has occurred. This group is used when a user from a blocked country logs in and the rule triggers and outputs a high alert.

■   **Block Action group** - The result of a rule is an action that is executed--what should take place--if the user logs in from a blocked country. In this case you block him and indicate to the client application to redirect the user to a page with an appropriate message "You Have Been Blocked."

### 12.22.7 Use Case: Allow Only Users from Certain IP Addresses

If the policy is to allow only users from IP Addresses that have been white listed as safe zones, you could create IP and Investigation Medium Alert groups:

- **IP group** - IP addresses are populated in a group type "IPs" that have been white listed as safe zones by an institution. Allow only users from IP Addresses that have been white listed as safe zones.

- **Investigation Medium Alert group** - Alerts are indicators to fraud analysts. Users who log in from IP addresses that are not in the white list group generate a medium alert. Alert type to Investigation.

### 12.22.8 Use Case: Check Users from Certain Devices

If the policy is to check users from devices reported for fraudulent activities, you could create Device and Information Alert groups:

- **Device group** - Devices that have been identified as suspicious are populated in a group type "devices." The devices are basically IDs that are generated based on many attributes such as browser, characteristics, flash, cookie, and so on.

- **Information Alert group** - Alerts are indicators to fraud Analysts. When a user from a device that is identified as fraudulent active [registered in the device group] logs in the rule triggers and outputs an information type alert.

### 12.22.9 Use Case: Monitor Certain Users

If the policy is to monitor users who have been reported for fraudulent activities, you could create User ID and Customer Care Alert groups:

- **User ID group** - Users who have been identified for fraud activity are populated in a group of type "User ID."

- **Customer Care Alert group** - Alerts are indicators to fraud Analysts as well as for Customer care representatives. When a suspicious user logs in the rule triggers and outputs a customer care alert.

## 12.23 Best Practices

This section outlines some best practices for using groups.

- Do not set the Cache Policy to "Full Cache" if you are using the group only for reports or for a group that is only collecting members and not used in any evaluation. For example, you should not cache a group if you have a long list of elements since groups are re-cached if there are any changes to the group.

- Ensure that the caching is set to "Full Cache" for action and alert groups.

# 13

# Managing the Policy Set

This chapter explains the management and use of the policy set in Oracle Adaptive Access Manager.

This chapter contains these topics:

## 13.1 Introduction and Concepts

This section introduces you to the concept of policy set and how it is used in Oracle Adaptive Access Manager. It includes the following sections:

### 13.1.1 Policy Set

The policy set is a level of evaluation logic above the individual policies. The policy set logic is a collection of functionality that executes after all the policies have executed for a checkpoint. This functionality includes the calculation of the final risk score and any overrides.

The policy set can be used to create action or score based overrides. The overrides allow an administrator to account for special circumstances where the actions or score generated by the policies may have an undesired effect. For example, to prevent a call center from being swamped by calls if a rule is configured too conservatively, an administrator can create an action override to convert a "Block" action if there are an extremely high number of blocks in a short period of time.

The policy set has a few key features:

- The scoring engine used to combine the scores generated by the individual policies into the final risk score is configured here.

- It can be used to create an action or a score override.

### 13.1.2 Action and Score Overrides

Action and score overrides can be used to change the outcomes of a checkpoint.

When you create an Action Override, you specify an 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 time frame.

When you create a Score Override, you specify an action group, or an alert group, or both to be triggered when the final risk score for a checkpoint falls within the specified range. For example, if you set the score range to 500 - 1000 and specify an alert group, the alerts are generated if the checkpoint risk score falls between 500 and 1000.

### 13.1.3 Before You Begin

Oracle Adaptive Access Manager is shipped with action overrides disabled (default). If you want this feature enabled, set the following property to "true."

```
vcrypt.tracker.rules.allowControlledActions
```

## 13.2 Navigating to the Policy Set Details Page

Only one policy set is available.

To access the **Policy Set Details** page:

1. Expand the Navigation tree.

2. From the Navigation tree, select **Policy Set**.

**Policy Set Details** is displayed.

Alternatively, you can open the **Policy Set Details** page by:

- Right-clicking **Policy Set** in the Navigation tree and selecting **Open Policy Set** from the context menu.

- Selecting **Policy Set** in the Navigation tree and then choosing **Open Policy Set** from the **Actions** menu.

- Clicking the **Open Policy Set** button in the Navigation tree toolbar.

## 13.3 Viewing Policy Set Details

The **Policy Set Details** page enables you to view and edit the details of a policy set.

It provides the following four tabs:

- **Summary** - Shows general details of the policy set and enables you to edit the details and select a scoring engine.

- **Score Overrides** - Enables you to set a score override

- **Action Overrides** - Enables you to set an action override

## 13.4 Adding or Editing a Score Override

To add or edit a score override:

1. Navigate to the **Policy Set Details** page.

2. Click the **Score Overrides** tab.

   A list of existing score override appears.

3. To add a score override, click **Add**.

   To edit a score override, select the override and click **Edit**.

   The **Add Score Override** or **Edit Score Override** dialog appears.

4. Select the checkpoint you want this override to be applied to.

5. Enter the minimum and maximum scores.

   The override triggers if the score falls between the minimum and maximum scores.

6. Select the action that you want triggered in an override.

7. Select the alert to which you want triggered in an override.

8. Click **Apply**.

## 13.5 Adding or Editing an Action Override

To add or edit an action override:

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

1. Navigate to the **Policy Set Details** page.

2. Click in the **Action Overrides** tab.

   A list of existing action overrides appears.

3. To add an action override, click **Add**.

   To edit an action override, select the override and click **Edit**.

   The **Add Action Override** or **Edit Action Override** dialog appears.

4. Select the checkpoint you want this override to be applied to.

5. In the **From Action** field, select the action that you want replaced.

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

   Specifying the **To Action** is optional. The **From Action** and **To Action** can be same.

6. In the **To Action** field, select the action you want to use for the replacement.

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

7. From the **Alert Group** list, select the alert 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.

8. For **Duration**, 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 stops blocking people and starts challenging those people who would have been blocked.

9. For **Count**, enter the number of events generated by the From Action.

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

   The count of the actions are incremented only if the action is from a different user, IP, and device.

   The count is updated only when the user, IP, and device are *all* unique. For example, if these are not unique and if a device is blocked, the device continues to be block in the specified duration instead of being challenged.

10. Click **Apply**.

# 13.6 Editing a Policy Set

To edit a **policy set**:

1. Navigate to the **Policy Set Details** page.

2. To edit the policy set's general information, make the changes you want in the **Summary** tab and then click **Apply**.

   You can change the **Policy Set'**s scoring engine and description.

   For information on Scoring Engines, see Chapter 14, "Using the Scoring Engine." OAAM Admin uses the scoring engine to calculate the numeric score applied when calculating risk level.

   If the changes are successful, a confirmation that the policy set details have updated successfully appears.

3. To add or edit the score overrides, follow the instructions in Section 13.4, "Adding or Editing a Score Override."

4. To edit the action overrides, follow the instructions in Section 13.5, "Adding or Editing an Action Override."

# 13.7 Use Cases

This section describes example use cases for using policy set.

### 13.7.1 Use Case: Policy Set - Overrides

William is a Security Administrator and he must set the score and action overrides such that when the score is between 500 and 700 for Pre-Authentication, a special alert is triggered for immediate attention by the fraud investigators and the users are "blocked instead of being "challenged."

1. Edit Score Override

When you create a Score Override, you specify an action group, or an alert group, or an action and an 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.

   **a.**  Checkpoint: **Pre-Authentication**

   **b.**  Minimum score: **500**

   500 is the minimum score allowed before the score override is triggered.

   **c.**  Maximum score: **700**

   700 is the maximum score allowed before the score override is triggered.

   **d.**  Alert Group: **new alert**

   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.

   **e.**  Action Group: **Block**

   Oracle Adaptive Access Manager does not allow the user to access the system if he is blocked.

**2.**  Edit Action Override

When you create an Action Override, you specify an 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 time frame.

   **a.**  Checkpoint: **Pre-Authentication**

   **b.**  From Action: **Challenge**

   **c.**  To Action: **Block**

   **d.**  Alert Group: **new alert**

## 13.7.2  Policy Set - Overrides (Order of Evaluation)

William is a Security Administrator and he must set the score and action overrides such that when the score is between 500 and 700 for Pre-Authentication, a special alert is triggered for immediate attention by the fraud investigators and the users are "blocked instead of being "challenged." But there are about 10 training folks and they are given temp allows for the next 1 week. How do the action and score overrides affect these users?

**1.**  Edit Score Override

When you create a Score Override, you specify an action or alert group, or an action and an 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.

   **a.**  Checkpoint: **Pre-Authentication**

   **b.**  Minimum score: **500**

   500 is the minimum score allowed before the score override is triggered.

     **c.** Maximum score: **700**

     700 is the maximum score allowed before the score override is triggered.

     **d.** Alert Group: **new alert**

     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.

     **e.** Action Group: **Block**

     Oracle Adaptive Access Manager does not allow the user to access the system if he is blocked.

**2.** Edit Action Override

When you create an Action Override, you specify an 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 time frame.

     **a.** Checkpoint: **Pre-Authentication**

     **b.** From Action: **Challenge**

     **c.** To Action: **Block**

     **d.** Alert Group: **new alert**

**3.** Create **Training Folks** group.

**4.** Select group in **Exclude group** of **Pre-conditions** of all **Challenge** rules.

## 13.8 Best Practices for the Policy Set

This section outlines some best practices for using policy sets.

- Before you import a policy set into a production system, you should be aware that you are about to replace the entire system configuration in the production system. Export the current policy set before the actual import since you do not want to lose the current configuration. If the import fails or if there are any other issues that you did not anticipate. After you have imported the policy set, there is no way for you to perform an undo. When you have a backup available, you can import that configuration into your system immediately if the import fails.

- Only when an export is successful, should you import the policy set from the offline system into the online system.

- When the configurable actions are exported with a policy set. You should copy the Java classes to the specified directory after the import so that the configurable actions are not broken when they are imported back into a system.

# 14

# Using the Scoring Engine

Oracle Adaptive Access Manager uses scoring engines to calculate the risk associated with access requests, events, and transaction.

Scoring engines are used at the policy and policy set levels. The Policy Scoring Engine is used to calculate the score produced by the different rules in a policy. The Policy Set Scoring Engine is used to calculate the final score based on the scores of policies.

Where there are numerous inputs, scoring is a able to summarize all these various points into a score that decisions can be based on.

This chapter describes how the scoring engine calculates scores.

## 14.1 Concept of Scores

Oracle Adaptive Access Manager incorporates risk scoring into its decision making. When a user logs in to the online application, Oracle Adaptive Access Manager evaluates dozens of criteria. The transaction is scored according to their level of risk. The scores are then used to calculate a final score. Institutions can determine the level of risk they are willing to accept. Then, all the scores are used to calculate the final score as a summary.

Important term that you should know about are listed in this chapter.

### 14.1.1 Score

Score refers to the level of risk that has been calculated for specific situations or parts of a situation, expressed as a number.

The score is a number configured by the user that is assigned to a rule when the rule evaluates to true. The user can configure a scoring engine that is used to combine the scores of the rules in a policy and assign a score to the policy. The scores from various policies are combined using a policy set level scoring engine.

Higher scores indicate higher risk. The maximum score is 1000. The lowest score is 0, which means that the situation is safe.

### 14.1.2 Weight

Weight is a percentage value used to influence the total score. Policies have default weights. Weight is only used when a given policy or checkpoint uses a "weighted" scoring engine.

The Weighted Scoring Engines uses weights from subcomponents. For example, if you choose the Weighted Scoring Engine at the policy level, Oracle Adaptive Access Manager uses the weight specified for each rule level when calculating the policy

score. Similarly, when you choose a weighted scoring engine at the policy set level, Oracle Adaptive Access Manager uses weights specified for each policy.

The range is 0 to 1000.

### 14.1.3 Rule

A rule defines datapoints for suspicious patterns or practices, or specific activities, and the outcome when the pattern, practice or specific activity is detected. The possible outcomes of a rule are actions, a list of actions, alerts, a list of alerts, and a score. A rule score is always calculated; the other outcomes are optional.

### 14.1.4 Policy

A policy is a collection of rules specifically assembled and tuned to run inside a specific checkpoint and at a single time.

The policy score is evaluated from the score results of the policy's rules.

#### Note for Policies Migrated from 10*g* to 11*g*

Only security policies are available in 11*g*. Business, third-party, workflow policy types have been removed from Oracle Adaptive Access Manager.

In 11*g*, all policies are treated as security policies.

### 14.1.5 Policy Type

The concept of policy type has been removed from the product. All policies are treated as security policies in 11*g*.

### 14.1.6 Checkpoint

Checkpoints are the points before and during the session when specific rules are run to evaluate the risk for the user actions. There are multiple policies under one checkpoint. The scores of these policies are used to determine a score for the checkpoint.

Oracle Adaptive Access Manager performs a separate evaluation for each checkpoint and provides a score for each. The score for a particular checkpoint must be between 0-1000.

The checkpoint score is evaluated from the score results of its policies.

### 14.1.7 Policy Set

A policy set is a logical collection of policies that has been used to assess risk at checkpoints.

There is one Policy Set per application.

Through the Policy Set you can specify the scoring engine and the weight multiplier you want to use for evaluating risk for the checkpoints.

### 14.1.8 Scoring Engines

A scoring engine is provided at the policy level and at the checkpoint level.

The policy scoring engine is applied to rule scores to determine the risk for each policy.

The policy set scoring engine is applied to the scores of the policies under a checkpoint to determines the score for the checkpoint. The default scoring engine at the checkpoint level is "Aggregate."

*Table 14–1    Scoring Engines*

| Scoring Engine | Description |
|---|---|
| Maximum | Use this engine when you want to score based on the single rule with the highest level of risk. The rule and policy weights are not used by this scoring engine. |
| Minimum | Use this engine when you want to score based on the single rule with the lowest level of risk. The rule and policy weights are not used by this scoring engine. |
| Aggregate | Similar to a percentage evaluation for what rules triggered versus the total number of rules. Use this engine when you do not want to score based on any single rule but instead want to make one based on the average level of risk computed based on the number of rules triggered. The rule and policy weights are not used by this scoring engine. Total score of triggered rules divided by the total number of rules |
| Average | Use this engine when you do not want to score based on any single rule but instead want to make one based on the average level of risk found. The rule and policy weights are not used by this scoring engine.Total score of triggered rules divided by the total number of triggered rules |
| Weighted Average | Use this engine when you do not want to score based on any single rule but instead want to make one based on the average level of risk found. The weights in this case would be determined by how much each rule or policy indicates a risky situation. |
| Weighted Maximum | Use this engine when you want to score based on the single rule with the highest level of risk. The weights in this case would be determined by how much each rule or policy indicates a risky situation. |
| Weighted Minimum | Use this engine when you want to score based on the single rule with the lowest level of risk. The weights in this case would be determined by how much each rule or policy indicates a risky situation. |

## 14.2  How Does Risk Scoring Work?

To determine a risk score, each level applies its scoring engine to the results from one level below.

Checkpoint = Policy A + Policy B +Policy C

Policy = Rule A + Rule B + Rule C

Policy C = Policy D + Policy F (if nested policies)

1.  Each triggered rule returns a score.

    Each rule has its own default score and weight. The score and weight are used for the calculation of the rule score.

    The alerts configured at the rule level are propagated to the final level.

2.  Each policy returns a score.

    To obtain the policy score, the policy scoring engine is applied to the scores of the rules underneath.

    If the policy does not use a "weighted" scoring engine, the scores of the individual rules are used in determining the policy score.

    If the policy uses a "weighted" scoring engine, a percentage value is applied to the individual rule scores before the policy score is determined. The "weight" is specified in the policy.

In Figure 14–1, if a weighted policy scoring engine is used, the score for Policy A would be:

Scoring Engine (Rule A * weight, Rule B * weight)

For example, if the policy scoring engine is "Weighted Maximum Score" and the policy weight is 50% and if Rule A returned 1000 and Rule B returned 500, the policy score for Policy A is 500.

Policy A = Maximum of (1000* 50%, 500*50%)

Policy A = Maximum of (500, 250)

Policy A = 500

3. The checkpoint returns a score

The checkpoint score is determined by applying the policy set scoring engine to the score result of the policies underneath the checkpoint.

The default scoring engine at the checkpoint level is Aggregate.

The checkpoint score and the action is the final score and action returned.

All the alerts are propagated from rule configurations.

*Figure 14–1  Scoring*
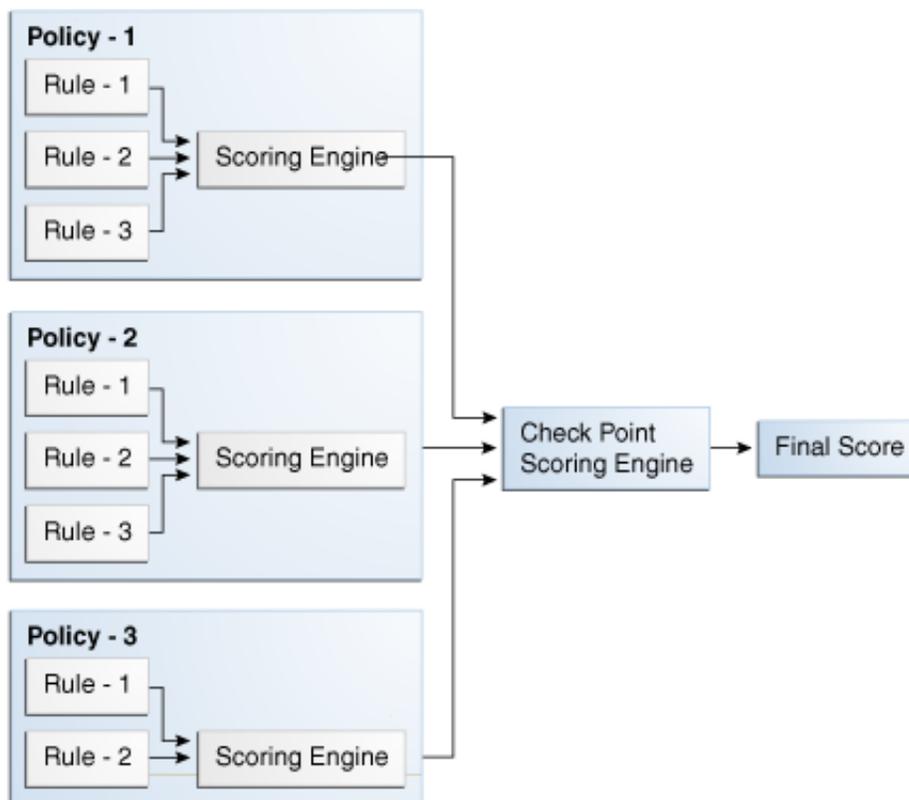


## 14.2.1 Score Propagation

Risk scoring (risk assessment) is useful in detecting the probability of fraud or business scenarios and in decision making. Oracle Adaptive Access Manager provides risk scoring at many levels and multiple gateways (checkpoints). From an aggregate of

the risk scores, the Rules Engine generates a single, high-level risk score to evaluate the total risk of a transaction.

There are multiple policies under one checkpoint. There are multiple rules under one policy. A score is determined at the policy level and then at the checkpoint level.

*Figure 14–2   Score Propagation*



The result from the 1st level is used to determine the result for the 2nd level and so on until the final level is reached.

Scores at these levels are determined by applying the scoring engine from these levels to the scores a level below.

For example, to determine the policy score, the scoring engine of the policy is applied to the scores of the rules within the policy. To determine the checkpoint score, the scoring engine of the checkpoint is applied to the scores of the policies within the checkpoint.

The checkpoint score and action are the final score and action in the assessment. The alerts are propagate from the rules level to the final level.

## 14.2.2 Nested Policies

Nested policies are evaluated based on scoring overrides. If the trigger combination itself is a policy, the score for the parent policy is retained, and the new policy gets its own score to be used for the evaluation of the checkpoint. If m1 has two rules, r1 and r2, and in the trigger combination, r1 contains m2. If the override triggers, r1 is used to calculate m1's score, and m2 is evaluated and used in the evaluation of the checkpoint. In calculating a score for the policy set, the score from m1 is used and the score from m2 is evaluated and used for the checkpoint score.

## 14.2.3 Scoring Override

Score overrides are used within a policy and within a policy set.

In policies, score overrides are specified in trigger combinations. Each rule has scores assigned. In trigger combinations, you can specify scores that are different from the defaults for the rules. Then, if the trigger combination is executed (triggered), the score of the trigger combination places the default score. If the trigger combination does not trigger, then the default score is used.

In a policy set, you can create a score override in which you specify an action group, or an alert group, or an action and an alert group you want to be triggered when a score falls within a specific range.

## 14.2.4 Action and Alert Overrides

You can create an Action or Alert Override to specify the action or alert to triggered as a final alert or action for a checkpoint.

# 14.3 Score Calculations

Policy score and checkpoint score are described in this section.

## 14.3.1 Policy Score

The different types of policy scores are listed in this section.

### 14.3.1.1 Aggregate Score

Sum of the scores of all triggered rules divided by count of rules.

### 14.3.1.2 Average Score

Sum of the scores of all triggered rules divided by count of triggered rules

### 14.3.1.3 Maximum Score

Higher score out of all triggered rules

### 14.3.1.4 Minimum Score

Lower score out of all triggered rules

### 14.3.1.5 Weighted Average Score

Sum of the scores (Score * weight modifier specified by the policy) of all triggered rules divided by the count of all rules

### 14.3.1.6  Weighted Maximum Score

larger score (S * weight modifier specified by the policy) out of all triggered rules

### 14.3.1.7  Weighted Minimum Score

lower score (S * weight modifier specified by the policy) out of all triggered rules

## 14.3.2  Checkpoint Score

The different types of checkpoint scores are listed in this section.

### 14.3.2.1  Average Score

Sum of the scores of all policies within the checkpoint divided by the count of all policies

### 14.3.2.2  Maximum Score

Higher score out of all policies

### 14.3.2.3  Minimum Score

Lower score out of all policies

### 14.3.2.4  Weighted Average Score

sum of policies (S* weight multiplier specified by the policy set) within the checkpoint divided by count of all policies

### 14.3.2.5  Weighted Maximum Score

larger score out of all policies (s* weight multiplier specified by the policy set)

### 14.3.2.6  Weighted Minimum Score

lower score out of all policies (s* weight multiplier specified by the policy set)

# 14.4  Best Practices

This section outlines a few examples on when certain scoring engines are used.

### Using a Maximum Scoring Engine

Whether a high score or low score is considered "bad" is dependant on the policy and how the developer models the policy. For example, the higher the score in device policies, the higher the risk for the situation.

For example, if you want "1000" to be considered a "bad" score, use the Maximum scoring engine. Then, model the rules so that whatever generates a maximum score is "bad." For example, you can model the policy such that if a user logs in from a particular location, the score is 200 points, and if a user logs in from a bad device, the score is 500 points. In this case, the one that has the maximum score is considered the worse of the two.

### Using an Aggregate Scoring Engine

If you do not know how risky a situation is, you can use an aggregate scoring engine. For example, for a Device ID, you can apply six or seven rules. For each rule, specify a score of 200 or 300 weight. If you the scores are more than this, it is considered "bad." If there are six rules, and two of them trigger, you would get the lower aggregate. If six

rules triggers, you get the higher aggregate, which means that this situation is the riskier.

**Using an Average Scoring Engine**

Use the Average scoring engine when none of the rules are more important than the others or there are a lot of rules that trigger for the evaluation. For example, each rule can view a particular part of a situation, but each part is not enough for you to base a decision on.

**Score Does Not Matter for Some Policies in a Checkpoint**

If there are multiple policies in a checkpoint and if the score does not matter for some of the policies, set the rule score to 0 for these policies, so that they are ignored when scores are aggregated.

# 15

# Creating Checkpoints

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

New checkpoints can be added and existing checkpoint properties can be modified using the Properties Editor.

This chapter provides information on how to create and configure a new checkpoint and how to modify an existing checkpoint.

## 15.1 Creating a New Checkpoint

To create a new checkpoint, use the Properties Editor.

The enumeration for a checkpoint is shown below for your reference.

```
profile.type.enum.<nameofcheckpoint>=<Checkpoint Value>
profile.type.enum.<nameofcheckpoint>.name=<Checkpoint Name>
profile.type.enum.<nameofcheckpoint>.description=<Checkpoint Description>
profile.type.enum.<nameofcheckpoint>.ruleTypes=user,device,location
profile.type.enum.<nameofcheckpoint>.listTypes=vtusers
profile.type.enum.<nameofcheckpoint>.finalactionrule=process_results.rule
profile.type.enum.<nameofcheckpoint>.isPreAuth=true
```

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

The Checkpoint name must be user-presentable and meaningful. The name is used in Oracle Adaptive Access Manager.

If the checkpoint creation is successful, add the appropriate properties by clicking the Add New button under the Properties box.

The Checkpoint's 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 checkpoint, 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 checkpoints.The out-of-the-box "process_results.rule" file is sufficient for most actions.

- listTypes= vtusers

  Always set listTypes to "vtusers."

The policy can be linked to only usergroups.

■ ruleTypes= user,device,location,in_session

The "ruleTypes" property defines the list of rule types supported during the checkpoint. Depending on the context of the checkpoint, 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 checkpoint.

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

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

Other properties you may add are:

■ isPreAuth

True indicates that this checkpoint is a pre-authentication checkpoint. OAAM Admin updates the user details with the pre-auth score and pre-auth action. The default for isPreAuth is "false." Note that there cannot be two checkpoints with this flag set to "true." Also the same checkpoint cannot be marked as postAuth and preAuth.

■ isPostAuth

True indicates that this checkpoint is a post-authentication checkpoint. OAAM Admin updates the user details with the post-auth score and post-auth action. The default for isPostAuth is "false." Note that there cannot be two checkpoints with this flag set to "true." Also the same checkpoint cannot be marked as postAuth and preAuth.

After creating the checkpoint, you need to restart the server.

## 15.2  Creating a Checkpoint Example

Below is an example for creating the "addressChange" checkpoint.

```
profile.type.enum.addressChange=88
profile.type.enum.addressChange.name=Address Change
profile.type.enum.addressChange.description=Address Change checkpoint
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
```

For finalactionrule, "process_results.rule" was provided because the Final Action for a given checkpoint 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.

# 16

# Managing System Snapshots

This chapter describes the Universal Risk Snapshot feature, which is new in Oracle Adaptive Access Manager 11*g*.

## 16.1 Concepts

This section introduces you to the concept of snapshots and how they are used in Oracle Adaptive Access Manager.

Using Universal Risk Snap shot, system snapshots can be created allowing security administrators to simply and easily migrate security data across environments or restore security configuration to a known state.

### 16.1.1 Snapshots

A snapshot is a backup of the current system configuration. In the event of an error on the original system, you can restore the system to a pre-defined point.

Universal Risk Snapshot only handle configuration data (metadata). It does not handle runtime data, such as sessions, transaction data, cases, rule logs, action logs, and others.

Universal Risk Snapshot enables System Administrators to store and manage a system image. They can:

- Back up the system configuration for safety, security, or versioning purposes

- Replicate the system configuration for use with other servers--for example, from test to production environment, for production troubleshooting, and others.

- Restore the system configuration from a pre-defined point

### 16.1.2 Snapshot Storage

When the snapshot is created, the OAAM Server metadata is copied from the database.

A snapshot can be restored from a file or from the database depending on where it was stored.

### 16.1.3 Snapshot Metadata

For snapshots, the metadata is stored with the following items:

| Artifact | Comments | Additional clarifications |
|---|---|---|
| Policy Sets | Policy Set overrides | |
| Policies | All Policies | Trigger combinations are included |
| Rule Instances | All rule instances | |
| Conditions | All rule conditions | |
| Groups | Group Definitions for all groups whether linked or not | Group Members for alerts and actions only will be exported |
| Patterns | All patterns | |
| Transaction Definitions | All transaction definitions | |
| Entities | All entities whether linked or not | |
| Properties | Only the ones in the database | |
| Enums | Only the ones in the database | |
| Configurable Actions | | |
| Challenge Questions | Includes validations, categories, and configurations (Answer Logic and others) | |

## 16.1.4 Backup

A backup saves all the existing configurations (both active and inactive items) including all group definitions. Only Action and Alert group members are included in the backup. Other group members can be exported using the group user interface if needed.

You can choose to create a backup snapshot in the database or to a local file system or both.

## 16.1.5 Restore

You can restore the new system configuration from a file or database.

Restore replaces the current system configuration with the restored configuration and also deletes and disables the additional configurations in the existing system.

> **Note:** The exception is when a group definition is imported into the system. The restore does not delete the additional group members that are already available.

- When you create a snapshot, all the configurations for functional areas are selected, both active and disabled. For example, if you have ten policies within your policy set, and five of them are active and five of them are disabled, all policies, their configuration, and their status information are included when the snapshot is created.

- Snapshots do not include the members of any groups with the exception of actions and alerts. However the groups themselves are included in the snapshot. To back up group members, the export groups function must be used separate from snapshot. These group members must be imported using the **Group** user interface if needed

- Though configurable action definitions are included on restore, you must ensure that the necessary java classes are manually copied into the required folders.

- The status of the items are preserved on backup and restore. For example. disabled items should remain disabled on backup and restore.

- You cannot selectively select individual items to include in a snapshot or perform selective restoration. If you only want to include certain configurations in your snapshot, you can export them from their module (separate user interfaces), and import them back and then create the snapshot.

### 16.1.6 How Restore Works

The metadata existing in the system is deactivated. Data cannot be deleted (policies or patterns) because it would violate database constraints. Therefore, all the active artifacts are set to an "inactive" or a "deleted" state as appropriate.

Afterward, the artifacts being imported are inserted into the current database.

During this insert process, if there are artifacts in the old system and also in the incoming snapshot, the artifacts are re-stored as they appear in the incoming snapshot.

Groups in the incoming snapshot do not contain members. If the same group exists (by name) in the existing system, after the system restore, the restored group contains members.

## 16.2 Navigating to the System Snapshot Search Page

To go to the System Snapshot Search page, perform the following steps:

1. Log in to OAAM Admin as a system administration.

2. In the Navigation tree, select **System Snapshots** under **Environment**.

   Alternative methods to open search pages are listed in

   On the **System Snapshot Search** page, you can perform the following tasks:

   - Search for a snapshot

   - Restore a snapshot from the database

   - Restore a snapshot from a file

   - Back up the current system to a file or database

   - Delete selected snapshots from the database

## 16.3 Searching for a Snapshot

In the System Snapshots Search page, you search for a snapshot by specifying criteria in the Search filter.

When the System Snapshot Search page first appears, the Search Results table shows a list of snapshots in the Oracle Adaptive Access Manager environment.

To search for snapshots:

1. In the Navigation tree, open **System Snapshots** under **Environment**.

   The **System Snapshots Search** page is displayed.

2. Specify criteria in the Search Filter to locate the snapshot and click **Search**.

- Searches are not case sensitive
- Searches can return results if you enter part of the name in the search.
- Searches trim the spaces entered.

Clicking **Reset** instead of **Search** will reset the search criteria.

The search result is shown based on the entered search criteria.

*Table 16–1    System Search Filter Criteria*

| Filter and fields | Description |
| --- | --- |
| Snapshot Name | Name of the snapshot. For a snapshot from a database, it is the name provided by the user; for file based backups, it is the file name. |
| | The snapshot with the specified name is displayed in the Results Table. |
| Notes | Notes describing why the snapshot was created. All backup names with the specified Notes keyword is displayed in the Results Table. |
| Backup date | Date at which the backup was taken. To locates a backup taken within a given create date range, enter the start and end dates you want for the range. All backup names that were backed up during the specified date range is displayed. |

## 16.4  Viewing Details of a Snapshot

To view details for a snapshot:

1. In the Navigation tree, select **System Snapshots** under **Environment**.

   The **System Snapshots Search** page is displayed.

2. Specify criteria in the Search Filter to locate the snapshot and click **Search**.

   Clicking **Reset** instead of **Search** will reset the search criteria.

3. Click the snapshot name in the **Results** table, the **Snapshot Details** page for the specific snapshot is displayed.

   The backup name, notes, system user, client IP, server IP, and server name for the backup is displayed in the **Summary** tab.

   The **Snapshot Preview** tab displays the configuration details for the following

   - Answer Hint
   - Question Category
   - Conditions
   - Validations
   - Questions
   - Groups
   - Policies
   - Entity Definition
   - Scheduler Task Group
   - Pattern

## 16.5 Creating a Backup

To create a backup:

1. In the Navigation tree, open **System Snapshots** under **Environment**.

   The **System Snapshots Search** page is displayed.

2. Click the **Backup** button on the right upper corner of the page or **Back up** from the Actions menu.

   The **Backup Current System** page is displayed.From this page, you can choose an option and provide the necessary information.

   The current system can be backed up to the system database or to a file or to both.

3. Select **Backup** type.

   - Database

   - Database and File

   - File

### 16.5.1 Backing Up the Current System to the System Database

To back up the current system to the system database:

1. From the **Backup Current System** page, select **Database** for the **Backup Type**.

2. Enter a name for the backup.

3. Enter notes for the backup.

4. Click **Back Up**.

   A dialog appears with a message that the current system has been successfully stored in the database.

5. Click **OK**.

   The system snapshot is created in the database.

### 16.5.2 Backing Up the System Configuration in Database and File

To back up the current system in a database and file:

1. From the **Backup Current System** page, select **Database and File** for the **Backup Type**.

2. Enter a name for the backup.

3. Enter notes for the backup.

4. Enter a file name for the ZIP file.

5. Click **Back Up**.

   A dialog appears with a message that the current system has been successfully stored in the database.

6. Click **OK**.

   The system snapshot is created in the database and file.

7. Verify that the snapshot is saved in database and file

   Search by the snapshot name in the **System Snapshots Search** page.

If backup is saved in the database, the snapshot name is listed in the results table.

### 16.5.3 Backing Up the Current System to a File

To back up the current system to a file:

1. From the **Backup Current System** page, select **File** for the **Backup Type**.

2. Enter a name for the backup.

3. Enter notes for the backup.

4. Enter a file name for the ZIP file.

5. Click **Back Up**.

   A dialog appears with a message that the current system has been successfully stored in the database.

6. Click **OK**.

   The system snapshot is created in the file.

## 16.6 Restoring a Snapshot

You can restore a system configuration from a snapshot of the same system or another system. You cannot choose to restore only a subset of the snapshot.

Restoring a snapshot replaces the system configuration completely.

If an error occurs during an operation, you can restore the system to a snapshot that predates the error.

### 16.6.1 Steps to Restore Selected Snapshot

To perform the restore operation:

1. Open **System Snapshot** under **Environment** in the Navigation tree.

   The **System Snapshots Search** page is displayed.

2. Click **Search** to populate the **Results** tab or search for the snapshot you want to use to restore the system.

3. Select a snapshot from the **Results** table.

4. Click **Restore** or select **Restore** from the **Actions** menu.

   A **Back Up Current Configuration** dialog appears, which offer you the option to back up the current system before replacing it. You can press **Back up**, **Skip**, or **Cancel**.

5. Enter a name for the backup.

6. Enter notes for the backup.

7. If you press **Back up** and the backup is successful, a message appears with a message that the current system was successfully stored in the database.

8. Click **Restore**.

   A summary displays a list of items being imported and the status of the operation.

9. Click **OK**.

An error message appears if the file was in the wrong format.

## 16.6.2 Loading and Restoring a Snapshot

To load a snapshot into the system database:

1. Open **System Snapshot** under **Environment** in the Navigation tree.

   The **System Snapshots Search** page is displayed.

2. Click the **Load from File** button.

   A Load and Restore Snapshot dialog appears for you to enter the name and notes for the current system configuration you are backing up in the database.

3. Enter the name and notes for the current system configuration and click **Continue**.

   The Load and Restore Snapshot dialog appears with a message that the current system has been successfully stored in the database.

4. Click **OK**.

   The Load and Restore Snapshot page appears for you to choose a snapshot to load.

5. Browse for a snapshot, and click the **Load** button to load the snapshot into the system database.

   If you press **Load**, the loaded snaphot is restored and becomes the current snapshot. If you select this option, you cannot preview the snapshot before restoring it.

6. Click **OK**.

7. Click **Restore**.

## 16.6.3 Snapshot Restore Considerations

Snapshot restore considerations are described in this section.

### 16.6.3.1 Snapshot in Live System (Single Server)

Snapshot ZIP files will have the server version from which it was taken. When re-storing if the version is determined to be in-compatible then the snapshot restore fails.

If the snapshot is restored in a system that is running, the effect is applicable in about 30 seconds when all the database artifacts are reloaded.

### 16.6.3.2 Snapshot Restore in Multi-Server System (Connected to the Same Database)

When the snapshot is restored in a system running with multiple servers connected to the same database, the snapshot is effective in approximately 20 seconds when servers reload their database artifacts.

All the servers are running on the same version of Oracle Adaptive Access Manager.

### 16.6.3.3 Snapshot Restore in Multi-Server Running Different Versions

The snapshot restore is checked by the server in which the restore was performed. If a server in a cluster is not compatible with the snapshot being restored, the server does not function since it is trying to read information from a database that it does not understand. The database schema might be compatible, but servers could differ in interpretation of features/ column value.

## 16.7 Importing a Snapshot

To import a snapshot for use in the system, follow the instructions in Section 16.6.2, "Loading and Restoring a Snapshot."

## 16.8 Deleting a Snapshot

To delete snapshots:

1. In the Navigation tree, select **System Snapshots** under **Environment**.

2. Click **Search** to view a list of snapshots in the system.

3. Select the snapshot to delete and click the **Delete** icon or **Delete Selected** from the Action menu.

   A Confirm Dialog appears with the message, "Are you sure you want to delete the selected Snapshot?"

4. Click **Delete**.

   A confirmation dialog appears with the message, "Selected Snapshots are deleted successfully."

5. Click **OK**.

## 16.9 Limitations of Snapshots

The following limitations apply to snapshots:

- Data that is not stored or restored is listed as:

  - Runtime data (examples: user-node logs, session and transaction logs, fingerprints, pattern collected data, generated alerts data, rule / policy logs data)

  - Geolocation data.

  - User action logs as related to server API logs

- The command-line utility is not available for this feature

## 16.10 Diagnostics

All the logs related to snapshot creation and restoration are contained in the server log.

## 16.11 Use Cases

This section describes example use cases for using snapshots.

### 16.11.1 System Snapshot Import/Export

Jeff a Security Administrator must migrate the policy changes and all dependent items from the test environment to the production environment.

1. Jeff goes into OAAM Admin in the test environment and exports the policy set

2. As part of the export process the policies, rules, conditions, linked patterns, linked groups (alert and action groups have members included by default. Other group types do not include member unless specified), enumerations used in policies,

transactions and entities used in the policies and configurable actions used in the policies are all selected for export to a file.

3. On import into the production environment a warning message alerts Jeff to the files that will be overwritten.

### 16.11.2 Use Case: User Exports Policy Set as a Record for Research

A snapshot is a record of how the rules and policies were configured; it contains the session information.

1. The user creates a snapshot so that historical data can be viewed later and research conducted using an offline system.

2. A timestamp is put on the snapshot.

3. Later, the user restores the older snapshot to perform fraud analysis.

4. The user runs rules and policies to find out how the system acted at that time in the past.

5. The user has multiple snapshots saved from different points in time and re-uses them in an offline system for performing research.

### 16.11.3 Use Case: User Replaces Entire System

A snapshot is a copy of the system configuration and contains the configuration for policies, rules, groups, and other elements in the system.

1. The user makes modifications to the policy set in the production system.

2. The user realizes that the changes were not the ones wanted.

3. The user restores the snapshot, replacing the entire system all together.

### 16.11.4 Use Case: User Identifies Policy Set to Import

The user is working on several snapshots offline, testing the rules and ensuring that the policies work as expected. He has finished work on SnapshotID 1 and SnapshotID 3, and he is now working on another configuration. Out of all the snapshots he has worked on, he wants to restore SnapshotID 3. He identifies SnapshotID 3 by Snapshot ID and restores it in the production system.

## 16.12 Best Practices for Snapshots

This section outlines some best practices for using snapshots.

- Before you perform a restore in a production system, you should be aware that you are about to replace the entire system configuration in the production system. Create a snapshot of the current policy set before the actual restore since you do not want to lose the current configuration if the restore fails or if there are any other issues that you did not anticipate. After you have restored the snapshot, there is no way for you to perform an undo. When you have a backup available, you can restore that configuration into your system immediately if the restore fails.

- Only when a snapshot is successfully created, should you restore the snapshot from an offline system to the online system.

- When the configurable actions are included with a snapshot. You should copy the Java classes to the specified directory after the snapshot creation so that the configurable actions are not broken when they are brought back into a system.

# Part V

## Autolearning

This part of the book contains instructions to configure the Autolearning, Configurable Actions, and Predictive Analysis features in Oracle Adaptive Access Manager.

It contains the following chapters:

# 17

# Managing Autolearning

Autolearning is a set of features in Oracle Adaptive Access Manager that dynamically profile behavior in real-time. The behavior of users, devices and locations are recorded and used to evaluate the risk of current behavior.

This chapter focuses on managing and using the Autolearning features in the following sections:

- Introduction and Concepts
- Before You Begin to Use Autolearning
- User Flows
- Navigating to the Patterns Search Page
- Searching for a Pattern
- Viewing Pattern Details
- Creating and Editing Patterns
- Importing and Exporting Patterns
- Activating and Deactivating Patterns
- Deleting Patterns
- Using Autolearning Data/Profiling Data
- Use Cases
- Pattern Attributes Operators Reference

## 17.1 Introduction and Concepts

This section introduces you to the concepts of autolearning and how they are used.

### 17.1.1 Autolearning

The Autolearning feature tracks transactions and authentications being performed by different actors based on patterns you create. This process establishes what is normal or average behavior for an individual or a population.

### 17.1.2 Patterns

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

Patterns require that bucketing, member types, and attributes to be defined. As well, rules must be configured to harness the profiling conducted by the patterns.

Patterns are used by Oracle Adaptive Access Manager to either define one bucket or dynamically create buckets. Oracle Adaptive Access Manager collects data and populates these buckets with members based on pattern parameters, and rules perform risk evaluations on dynamically changing membership and distributions of the buckets. Pattern evaluation and population occurs only when the result of the transaction is successful.

### Bucket Creation and Population

Figure 17–1 shows a bucket creation and population example.

*Figure 17–1   Login Times*
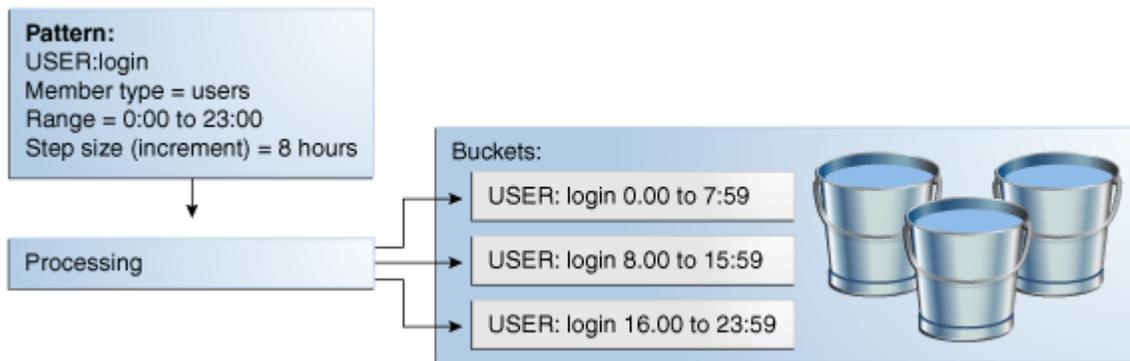


If you want to track employee login times, you would:

- Set up a pattern where the member type is **User** and the attribute is **Time**.

- Choose multi-bucket as the creation method for the pattern. A multi-bucket pattern creates as many buckets as required to capture behaviors as opposed to a single-bucket pattern which only creates one to capture a specific behavior.

- Set start time=0:00 and end time=23:59, which are the hours of the day, and a increment step size of 8 hours.

During the processing of the transaction/login data, Oracle Adaptive Access Manager creates the buckets as required and populates them with counts for each member. Each bucket automatically keeps from overlapping with each other based on the other buckets already in the system. As shown in Figure 17–1, Oracle Adaptive Access Manager builds a maximum of 3 buckets with 8-hour periods in which logins have occurred.

For example, if Jeff logs in at 8:27, his counter in the 7:00 and 14:59 bucket is incremented by one. If no user has ever logged into this system between 7:00 and 14:59 then Oracle Adaptive Access Manager also creates that bucket as part of the processing. This 7:00 and 14:59 bucket then is used to record login time behavior for all users going forward.

After creation, the buckets are populated with the logins of users that have fallen within each 8-hour time range.

Oracle Adaptive Access Manager only records that Jeff used this computer if he logs in successfully. This validates that what is recorded is most likely Jeff's real behavior and not a fraudulent attempt to log in using Jeff's credentials. The memberships and associated statistics are saved in each user profile.

### 17.1.3 Member Types and Attributes

To profile behavior, members and attributes are required.

Members and attributes act as a guide for Oracle Adaptive Access Manager to analyze data. Member is the actor in the system. Examples of actors are user, IP address used for logging in, and so on.

Attributes are the particular pieces of information associated with the activity being tracked. An example is the time of day for a login. Patterns collect data about members. If the member type is **User**, the pattern collects data about users.

In defining the Pattern you specify which data points you are interested in for the members.

For example, if Joe lives in San Francisco, logs into a protected application from home at 9:00 am on a Friday; **City**, **Time**, and **Day of Week** are attributes associated with the user, Joe. A pattern could be configured to capture all the city, time, and day of the week combinations Joe uses to log in. Or separate patterns could be created for time, city and day of the week to be evaluated together or independently. The configuration you choose is based on the business use cases.

If you are interested in profiling the cities that users log in from, the attribute to profile would be **City**.

Another example, if you want to track users based on the devices they use, you would set up a pattern with User as the member type since you want to collect information about users. You would then select Device ID as the attribute since you want to know the devices each user is using.

Because members and their attributes are tracked by Oracle Adaptive Access Manager when configured to do so, it is possible to capture complex behavior. However, often times the best practice is to keep the patterns relatively simple in terms of the number of attributes and then use rules to perform complex evaluations involving multiple patterns tracking different attributes. This strategy is more flexible and manageable in the long run.

### 17.1.4 Buckets

Patterns are configured by an administrator and Oracle Adaptive Access Manager uses that configuration to create buckets as it needs them. Administrators do not deal or see buckets directly in any way.

Patterns are configured to create either one bucket or multiple buckets. Buckets are containers that are used to capture the frequency of behaviors. Rules evaluate the counters in these buckets for specific members to determine if a situation is anomalous.

- Single-Bucket

    Single-bucket patterns 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 is created and populated with users. If a user logs in from the United States, he or she becomes a member of the bucket and the bucket counts are incremented; if he or she does not log in from the United States, the bucket count is not incremented.

    Another example, if you choose to create an authentication pattern for users (member type) with time 8am to 5pm (attribute), exactly one bucket is created and populated with users. If a user logs in from 8am to 5pm, he or she becomes a

member of the bucket and the bucket counts are incremented; if the user does not log in between 8am to 5pm, the bucket count is not incremented.

*Figure 17–2   Single Bucket*
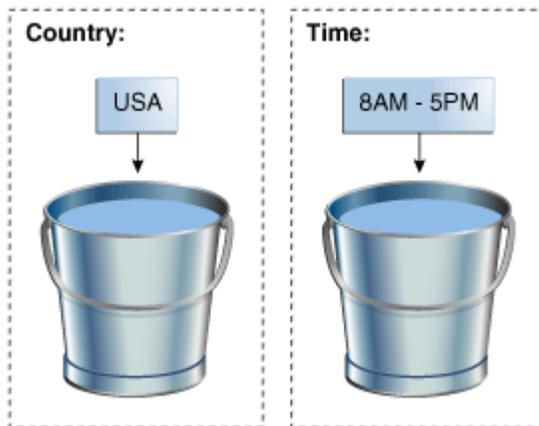


- Multi-Bucket

  Multi-bucket patterns usually create more buckets than single-bucket patterns. They create buckets as required based on the parameter configurations.

  You configure the data types and samples you want Oracle Adaptive Access Manager to generate buckets from, and then during pattern processing Oracle Adaptive Access Manager creates buckets as needed to capture behaviors.

  For example:

  – If you specify "For each" as the compare operator and country as the attribute, Oracle Adaptive Access Manager creates a bucket dynamically for each country as activity occurs from the country. The first time any user logs in from Canada, Oracle Adaptive Access Manager creates a Canada bucket and adds that user as a member with a count of one. The next user to log in from Canada is added to that same bucket as a member with a count of one. Each subsequent time a user logs in from Canada his Canada bucket counter is incremented.

*Figure 17–3   Countries Multi-Bucket*
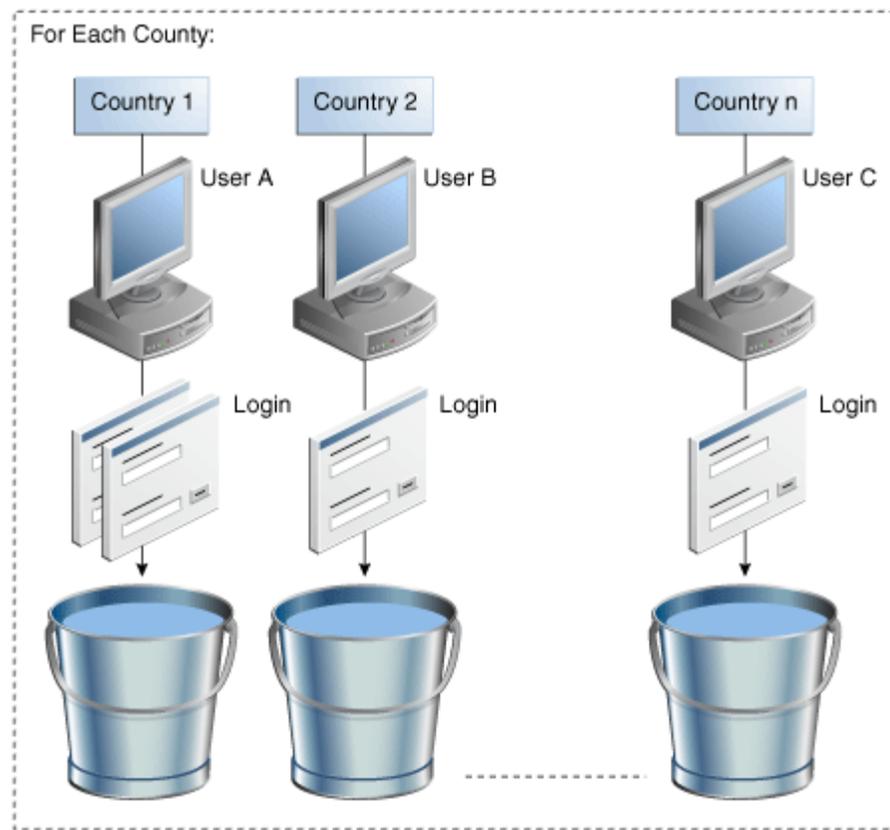


- Buckets are not created until they are needed. If you choose user logins for a 24-hour range with an increment step size of 8 then up to 3 buckets are created, one for each 8-hour time slot in which logins occur.

*Figure 17–4   Time Multi-Buckets*
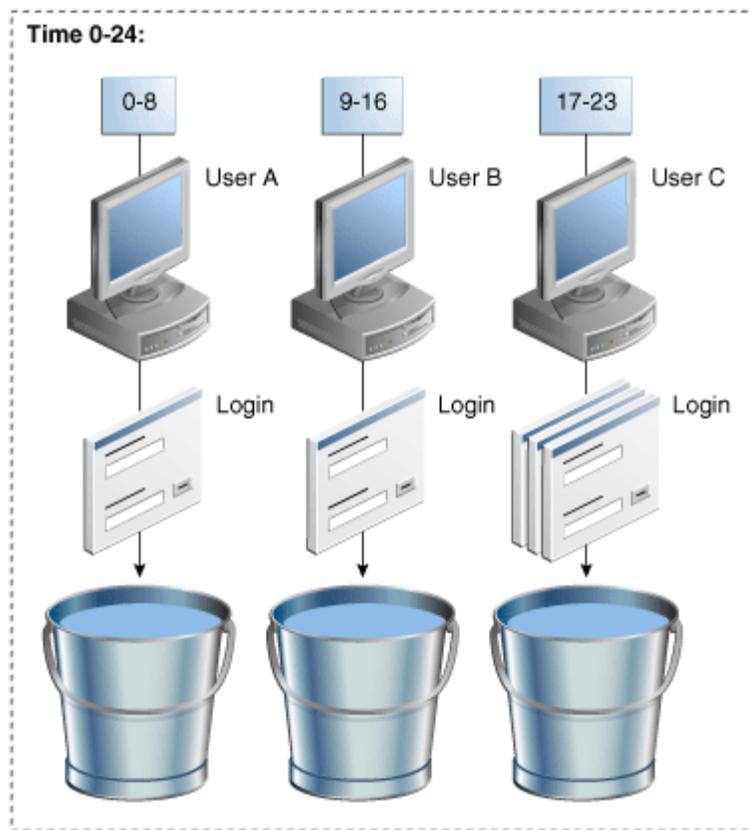


## 17.1.5 Pattern Rules Evaluations

OAAM uses patterns and the buckets they generate to capture the frequencies at which specific behaviors occur for each individual user, device, location, and so on. Since the pattern buckets are updating in real-time rules can be run against them to dynamically determine if the current behavior seems abnormal. The rules evaluations can view either the individual's current behavior versus his past behavior or the individual's current behavior versus the past behavior of all individuals.

The Autolearning feature tracks transactions and authentications being performed by different actors (entities) based on patterns you create. This process establishes what is normal or average behavior for an individual or a population.

Note: Transaction patterns can only be defined based on entity values and not data values.

**Figure 17–5   Bucket Evaluation**
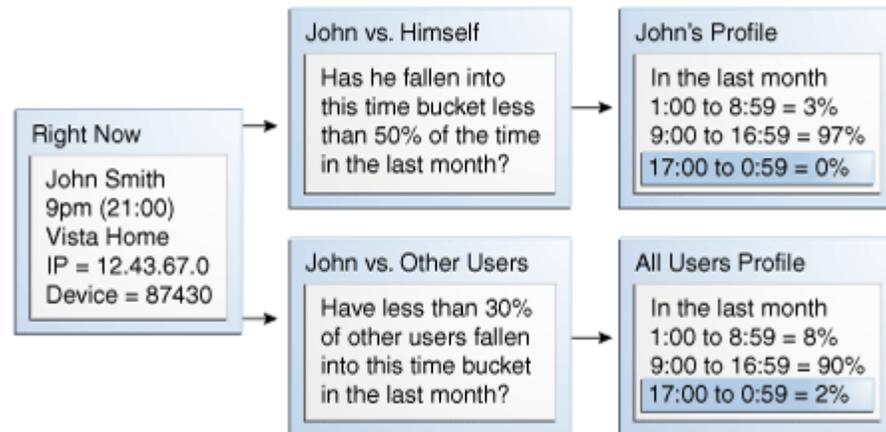


In this example John's login behavior is being evaluated against his own profile and the profile of all users.

### Bucket Evaluation Example

In this example a pattern was created to capture user, device and IP login time behavior. The multi-bucket pattern was configured to create buckets to cover the entire 24 hours of the day in four hour samples. Consequently, OAAM ended up creating four time buckets as login activity occurred within each time range.

| Buckets | Time Range |
|---------|------------|
| Bucket #1 | 0:00 to 4:59 |
| Bucket #2 | 5:00 to 8:59 |
| Bucket #3 | 9:00 to 16:59 |
| Bucket #4 | 17:00 to 23:59 |

After a month of recording, the system has created four time buckets and populated them with members and counters for each member. The three entities now have the following bucket memberships.

| Entity | Membership |
|--------|------------|
| User A | #3 |
| Device X | #2, #3, #4 |
| IP Y | #2, #3 |

Evaluation of the memberships produces the following conclusions:

> **Note:**   These scenarios are not a sequence; each is a distinct scenario.

| Scenarios | Risk |
|-----------|------|
| If User A logs in at 3:37 using Device X from IP Y | very high risk (none are in #1) |

| Scenarios | Risk |
|---|---|
| If User A logs in at 18:07 using Device X from IP Y | medium - high risk (device in #4) |
| If User A logs in at 8:27 using Device X from IP Y | medium risk (device and IP in #2) |
| If User A logs in at 11:15 using Device X from IP Y | very low risk (all in #3) |

The following paragraph describes the first scenario in more granular detail.

If User A logs in at 3:37 and he has previously only logged in between 9:00 and 16:59 that elevates the risk because he is not a member of the Bucket #1. If Device X is used and it has previously only been used between 5:00 to 23:59 that elevates the risk because User A and Device X are not members of Bucket #1. And, if IP Y is used and it has previously only been used between 5:00 to 16:59 that elevates the risk as well since User A, Device X, and IP Y are all not members of Bucket #1. Since all three of the major components involved in the risk evaluation are not in bucket #1 the overall risk level is very high. It is important to emphasize that each of these elements is evaluated for membership in the time profiles independently in this example.

### 17.1.6 Bucket Population

Buckets are created, populated and the counters incremented only after the transaction is successful.

**Example**

Joe logs in from three cities (home, office A and office B). A city pattern records how often he logs in from each.

| Bucket | Location |
|---|---|
| City Bucket #1 | home |
| City Bucket #2 | office A |
| City Bucket #3 | office B |

Joe's company wants users to be challenged with an OTP two sessions in a row if they are logging in from a city they have not used in the last month. If Joe stops working at office B for 37 days and does not access from anywhere else in that city he is challenged for an OTP the next time he logs in from that city. To accomplish this use case a rule is configured to check on the membership count for the current city bucket in the last month. The count threshold is set to two so the rule triggers until the user has been a member at least twice in the last rolling month window.

## 17.2  Quick Start for Enabling Autolearning for Your System

The chapter has been organized into sections by topic. If you have used autolearning before, use this chapter effectively in any order that is convenient for you.

If you want profiling and autolearning enabled in your system, follow this procedure:

1. Make sure entities are imported.

   See Section 17.3.1, "Importing Base Authentication-Related Entities."

2. Enable autolearning properties.

   See Section 17.3.2, "Enabling Autolearning Properties."

3. Import autolearning policies into the server.

4. Create patterns.

   Define patterns, add attributes, and activate /enable the patterns so that the system can start collecting pattern data.

   See Section 17.9, "Creating and Editing Patterns."

5. Finally, use the patterns in rule evaluation.

   For information on using autolearning, see Section 17.12, "Using Autolearning Data/Profiling Data."

   To verify that autolearning is turned on and working, see Chapter 31, "FAQ/Troubleshooting."

## 17.3 Before You Begin to Use Autolearning

Before using the Autolearning feature, read through Section 17.1, "Introduction and Concepts." The section is useful in helping you to understand the concepts presented in this chapter.

To use the Autolearning feature, you must perform the following procedures.

### 17.3.1 Importing Base Authentication-Related Entities

The actors that are tracked during authentication are called authentication entities and include user, city, device, and so on. These base entities are required to enable conditions that are used for patterns. Before you begin using the Autolearning feature, you must import these base entities into your system. Refer to Section 2.6, "Importing the OAAM Snapshot."

To import the entities into the server:

1. Navigate to the **Entities Search** page, as described in Section 20.2, "Navigating to the Entities Search Page."

2. Click **Import Entities**.

3. In the **Import Pattern** dialog, click **Browse** and locate **Auth_EntityDefinition.zip**.

4. Click **OK**.

   OAAM Admin shows the entities in that file.

5. Select and import all of them.

### 17.3.2 Enabling Autolearning Properties

Enable autolearning so that OAAM collects profiling data.

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

   The default value is true. It is like a "master (on/off) switch" for autolearning.

   If this property is absent, this default value is used. If the property is present, the assigned value is used.

2. Set the following properties to true:

   If the properties do not exist, create them.

   - vcrypt.tracker.autolearning.use.auth.status.for.analysis

This property must be set to true for the authentication patterns to work. Authentication patterns are the patterns that are used in processing the data relevant to authentication (login) related information only.

- vcrypt.tracker.autolearning.use.tran.status.for.analysis

This property must be set to true.

### 17.3.3 Importing Autolearning Policies into the Server

Import the out-of-the-box autolearning policies, refer to Section 2.6, "Importing the OAAM Snapshot."

### 17.3.4 Using Autolearning in Native Integration

Before autolearning can be used for monitoring of transactions and authentications, native integration clients need to use updateStatus or updateTransaction APIs which use the autolearning flags.

Alternatively native integration can also use the processPatternAnalysis API for processing the session data for autolearning.

The API helps to provide OAAM with information about user activity (logins or transactions). For example, updateAuthStatus or updateTransaction is called when a customer login is complete or a login is blocked, and so on.

For the UpdateAuth Status API, an analyzePatterns value of "true" triggers the pattern processing for the login. If no value is passed, a value of false is assumed. If the authentication status value, resultStatus, is "success" and the analyzePatterns value is "true," OAAM processes the users's data and autolearning/profiling data is collected for the user.

For any login, autolearning is performed only once if the authentication status is "success." If the authentication or transaction status is not "success," the buckets are not updated. If the buckets are not updated, the data that autolearning rules use may not be accurate.

For information on autolearning APIs, see Appendix B, "Pattern Processing."

## 17.4 User Flows

User flows are presented for:

- Creating a New Pattern
- Editing a Pattern

### 17.4.1 Creating a New Pattern

These steps describe the Create New Pattern flow:

1. Search for a pattern.

2. If pattern exists, view pattern details.

3. If pattern does not exist, create new pattern.

4. Specify pattern name, member type, evaluation priority, and description.

5. Add attributes.

If there are no validation errors, the new Pattern is created successfully.

### 17.4.2 Editing a Pattern

The following steps describe the Edit Pattern flow.

> **Note:** If you edit a Pattern the data that is already collected based on that pattern could potentially become unusable. For example, if a user edits a Pattern and removes one of the attributes, the data that was collected previously may not be usable since the buckets created in the past for this Pattern would have taken into account the attribute that is now being removed.

1. Search for a pattern.

2. If Pattern exists, view pattern details.

3. Change details.

4. Add attributes.

If there are no validation errors, the pattern is edited successfully.

## 17.5 Navigating to the Patterns Search Page

To navigate to the Patterns Search page:

1. In Fraud Prevention, expand the Navigation tree.

2. Double-click **Patterns**.

   The **Patterns Search** page is displayed with results based on the default search criteria.

   Alternative methods to open the search page are listed in Section 3.9, "Search, Create, and Import."

The **Patterns Search** page is the starting place for managing your patterns. From the **Patterns Search** page, you can:

- search patterns
- view a list of patterns
- create new patterns
- delete patterns
- activate patterns
- deactivate patterns
- import patterns
- export patterns

## 17.6 Searching for a Pattern

To search for a Pattern:

1. Navigate to the **Patterns Search** page, as described in Section 17.5, "Navigating to the Patterns Search Page."

   An example **Patterns Search** page is shown in Figure 17–6.

*Figure 17–6   Patterns Search Page*
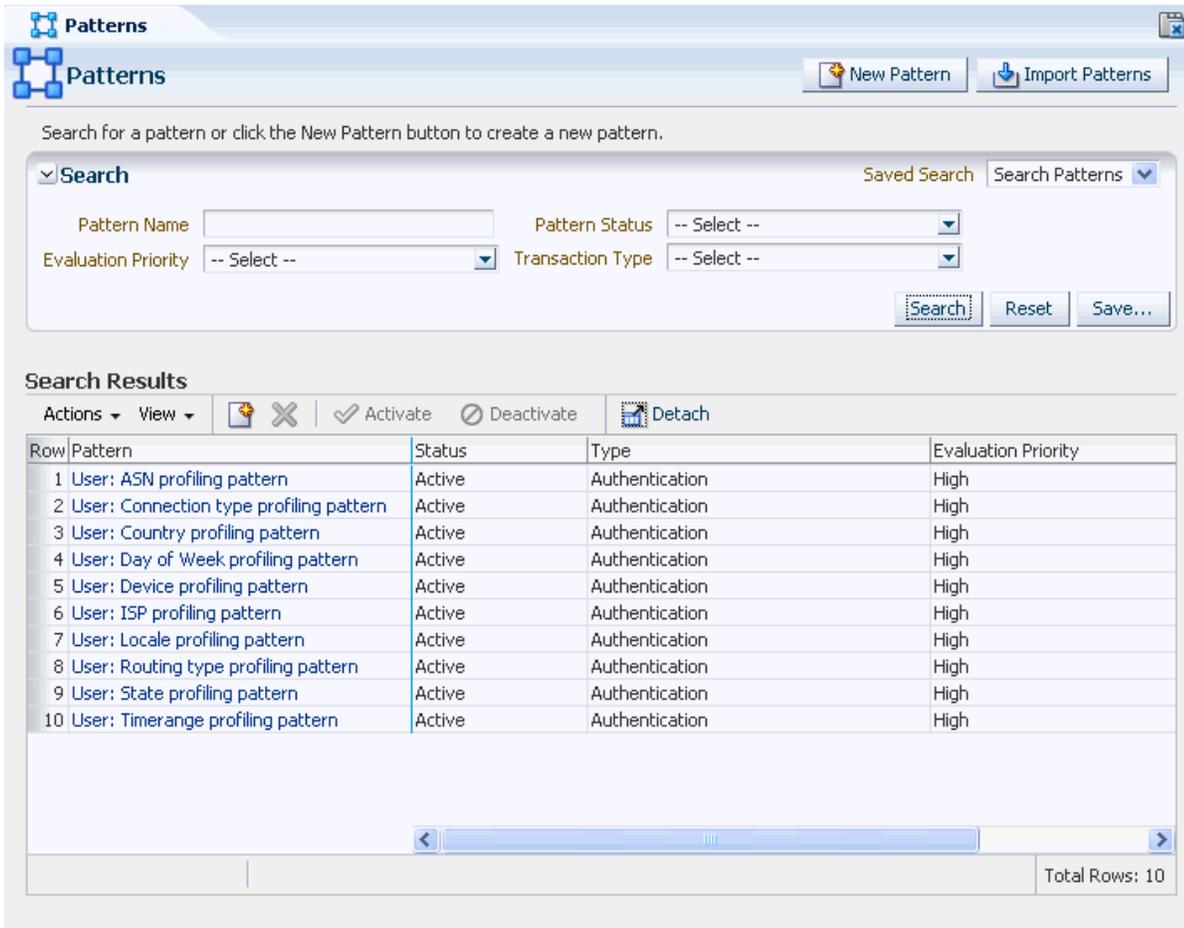


The **Pattern Search** page displays a Search section and a **Results** table that shows a summary of the patterns that match your search criteria.

**2.** Specify criteria in the Search Filter to locate the pattern and click **Search**.

The search filter criteria are described in Table 17–1.

If you want to reset the search parameters to the default setting, use the **Reset** button.

*Table 17–1  Search Filter Criteria*

| Field | Description |
|---|---|
| Pattern Name | The name of the pattern. You can enter the complete name or part of a Pattern name. |
| Evaluation Priority | The priority in which the collected data is evaluated.<br><br>■  High<br><br>Most of the resources are assigned for the data to be evaluated.<br><br>■  Low<br><br>The resources assigned to data evaluation is half as much as the High priority. |
| Pattern Status | The state of the pattern. These are the pattern states:<br><br>■  Active<br><br>If data must be collected, the pattern must be in the active state.<br><br>■  Inactive<br><br>If the pattern definition is complete, but you do not want to collect data, select "Inactive."<br><br>■  Incomplete<br><br>If pattern creation has started, but you need to save it for completion later, select "Incomplete." Data is not collected for this state.<br><br>■  Invalid<br><br>If there is a problem with the pattern, you can mark the pattern as invalid to signal other operators. No autolearning data analysis is performed for a pattern in this state.<br><br>■  Deleted<br><br>The pattern has been deleted, but system must keep this record to maintain data integrity. No autolearning data analysis is performed for the pattern in this state.<br><br>It is recommended that you do not use the **Deleted** status. This status may not be available in future releases. |
| Transaction Type | Default is Authentication (login). Transaction patterns can only be defined based on entity values and not data values. |
| Creation Method | The type of bucket the Pattern had been created as.<br><br>■  Single Bucket - Single-bucket patterns create and populate one bucket with the exact data points and value ranges specified in the pattern<br><br>■  Multi- Bucket – Multi-bucket patterns have buckets for sub-ranges of a parameter range |

The **Search Results** table displays a summary of patterns that match the criteria specified in the **Evaluation Priority**, **Pattern Name**, **Pattern Status**, and **Transaction Type** fields.

If you want the summary to include the creation method, select **Creation Method** from the additional fields list under the View drop-down list.

Clicking the **Pattern** column header sorts all the pattern names in ascending or descending order. Sorting is available for all columns.

A tool tip is available to display the complete description of a pattern if the description is not shown fully in the user interface.

## 17.7 Navigating to the Patterns Details Page

Follow these steps to navigate to a **Pattern Details** page.

1. If you are not on the **Patterns Search** page, follow the instructions in Section 17.5, "Navigating to the Patterns Search Page."

2. Search for the pattern of interest, by following the instructions in Section 17.6, "Searching for a Pattern."

   There is a link on the pattern name in the **Search Results** table.

3. Click the pattern name and the **Pattern Details** page for the specific pattern appears.

From **Pattern Details**, you can select the member type and change the pattern name, pattern status, evaluation priority, and description after the pattern is created; add attributes, and view the pattern usage points.

## 17.8 Viewing Pattern Details

This section provides details on viewing patterns.

### 17.8.1 Viewing Details of a Specific Pattern

By clicking the pattern name on the **Patterns Search** page, the **Pattern Details** page for the specific pattern appears. For instructions, see Section 17.7, "Navigating to the Patterns Details Page."

The **Pattern Details** page provides such general details about the pattern as the pattern name, status, member type, evaluation priority, and description.

The **Pattern Details** page provides the following three tabs:

- **Summary** - General details such as pattern name, status, transaction type, and so on

- **Attributes** - Displays attribute details such as definition, status, description and so on.

The number of attributes are displayed in the tab (in parenthesis).

## 17.9 Creating and Editing Patterns

This section explains how to create and edit patterns. It contains the following topics:

- Creating a Pattern
- Editing the Pattern
- Adding Attributes
- Editing Attributes
- Deleting Attributes

### 17.9.1 Creating a Pattern

**Best Practices for Autolearning and Pattern Creations**

Best practices for autolearning and pattern creations are:

- For autolearning configurations: Administrators should keep in mind that any tracking of behavior warrants computational power and storage space and be prudent in configuring the system for the most returns on the efforts.

- Best practices for pattern creation: When creating patterns, you must ensure that other patterns in your system are not already collecting the same kind of information. For example, if you create a pattern to collect login time information on user and IP, and then you create another pattern on user and login time, you are creating two patterns that are collecting the same information.

- Best practices to keep Oracle Adaptive Access Manager current and relevant given the evolving online security threats: autolearning technology automatically adjust to changing activity and behaviors. For example, autolearning profiles what normal behavior is for each user and all users. In this way security policies are dynamically adjusting in real-time to how users really acts rather than a guess at how they will act. In addition to the automated features it is recommended that security policy be reviewed on a regular basis to make sure they are behaving as expected.

- For heavy pattern usage: You might assign different evaluation priorities to various patterns. For example, you can set login patterns to High and other patterns to Low.

- For evaluation property: Ensure that you do not set "High" as the evaluation priority for all your patterns, since performance will be impacted by doing so.

**Procedure to Create a New Pattern**

Follow this procedure to create a new pattern.

All values except transaction type can be modified later in the **Pattern Details** page.

**Transaction type**, **Creation Method**, **Member Type**, **Evaluation Priority**, and **Description** are required fields.

1. Navigate to the **Patterns Search** page, as described in Section 17.5, "Navigating to the Patterns Search Page."

2. In the **Patterns Search** page, click the **New Pattern** button or the **New** icon.

   Alternative methods to open the **New Pattern** page are listed in Section 3.9, "Search, Create, and Import."

3. In the **New Pattern** page, enter the pattern name.

   A unique pattern name must be entered.

4. Select the transaction type.

   The default is **Authentication**.

   The support for transaction-based patterns is limited. Transaction patterns can only be defined based on entity values and not data value. (You cannot create a pattern using the data elements from the transaction itself, only from the data elements belonging to the entities.) You cannot create rules based on those patterns.

5. From the **Creation Method** list, select the method you want to use to create the pattern.

   - Single-Bucket

   - Multi-Bucket

6. Select a member type.

   The member type is the actor for which data must be captured.

   For example, if you select city as the member type, the pattern created collects city data.

7. Select a evaluation priority

   **Evaluation priority** is the priority in which data is evaluated. There are two evaluation priorities: **High** and **Low**.:

   - High

     There is double the amount of resources made available to process the pattern data in this category as compared to the "Low" priority.

     Resources include processing resources and database resources.

   - Low

     There is half the amount of resources made available to process the pattern data in this category as compared to the "High" high priority.

   The chances for finishing the processing of high priority pattern data are doubled the chances for finishing the low priority patterns.

8. Enter a description.

9. Click **Apply**.

*Figure 17–7   New Pattern*



The **Pattern Details** page is opened with the **Summary** and **Attributes** tabs.

If you try to create a pattern that already exists in the database, an error occurs.

If you try to create a pattern with the same members as another pattern, a message appears: "A pattern with the same member configuration already exists. Are you sure you want to create a new pattern? If you answer "yes," you are allowed to create the pattern.

The pattern is enabled upon creation and the **Pattern Details** page is displayed. You can edit or review the pattern.

Patterns can be created without any attributes.

**10.** Add attributes.

*Figure 17–8   Add Attribute*
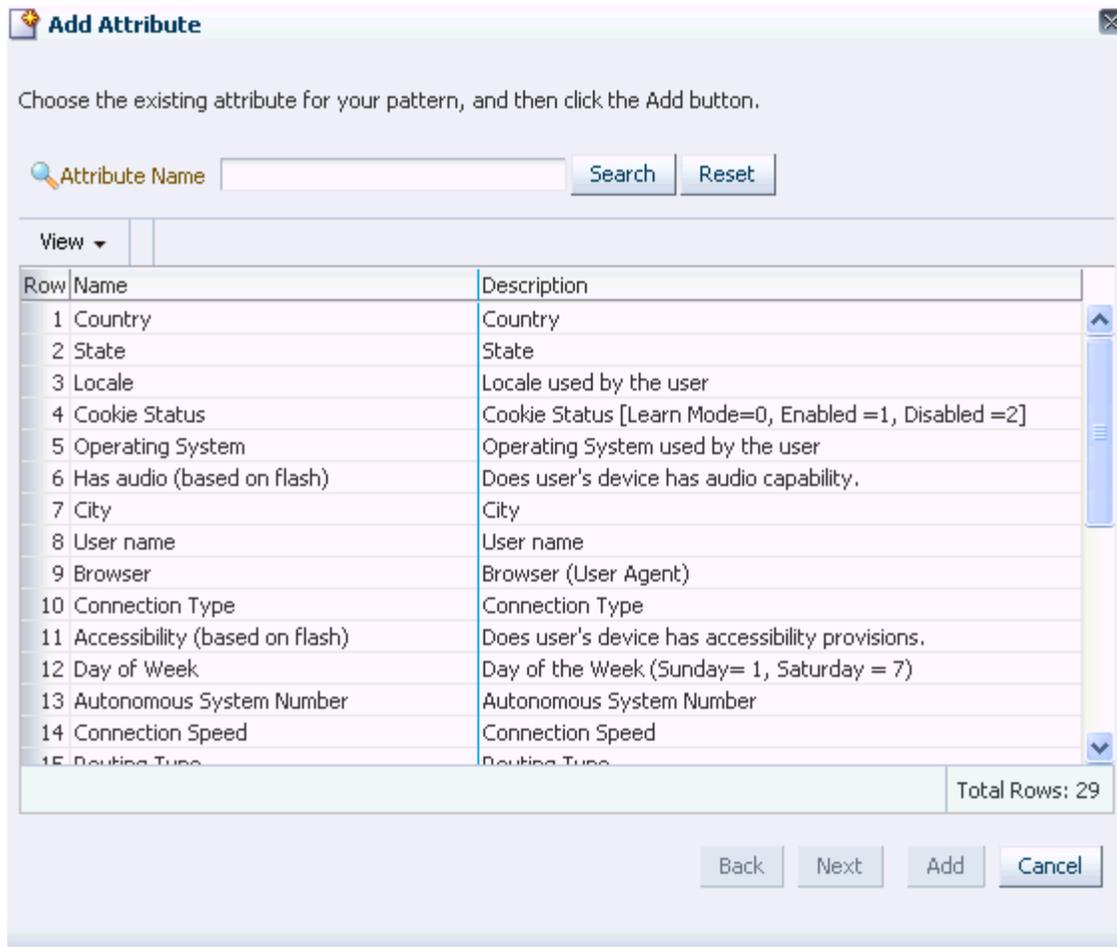


For information, see Section 17.9.2, "Adding Attributes."

For information on attributes, see Section 17.1.3, "Member Types and Attributes."

**11.** Activate the pattern.

To activate the pattern, see Section 17.9.3.1, "Activating Patterns."

To use the patterns in rule evaluation, see Section 17.12, "Using Autolearning Data/Profiling Data."

To verify that autolearning is working, see Chapter 31, "FAQ/Troubleshooting."

## 17.9.2  Adding Attributes

For information on attributes, see Section 17.1.3, "Member Types and Attributes."

Follow these steps to add attributes.

**1.** If you are not on the **Pattern Details** page of the pattern, follow the instructions in Section 17.8.1, "Viewing Details of a Specific Pattern."

**2.** In the **Attributes** tab, click the **Add** button in the **Search Results** toolbar.

**3.** In the **Add Attributes** dialog, select an attribute or attributes from the **Add** list.

Select attributes (data points) you are interested in for the member type. OAAM collects data on the attributes to determine if the member belongs to the profile.

For example, if you select "user" as the member type and the attributes: IP (NNN.N.N.N), City (Redwood City) and Is Registered (False); OAAM records when users match all of these attributes--the user has an IP address of NNN.N.N.N, who lives in Redwood City, and who is not registered. This profiling can then be used to evaluate risk for the "user."

For example, if you want OAAM to track the login times for "user" and "IP" (member type), you would select "time" as an attribute.

After the attributes are added, they are not available in the list for further selection.

4. Specify the condition information for the attribute.

   a. Select the **Status**.

      For example, "Active" if you want OAAM to collect data on the attribute to be used in the pattern membership.

   b. Enter the description.

      For example, "This pattern creates buckets to track login times for users and IPs."

   c. Select a compare operator.

      For example, "range" with start value of 0 and end value of 23 if you want to collect data for a range of 24 hours.

      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.

      For detailed information about compare operators, see Section 17.19, "Pattern Attributes Operators Reference."

   d. Enter **Increment Step**.

      The sample size (interval)

      For example, 2 for 2 hour intervals.

   e. Click **Add**.

5. In the **Attributes** tab, use the arrow controls to reorder the attributes if you want.

   Order is not required and is automatically pre-filled.

6. Click **Apply**.

   A dialog appears, with the message that the attribute was added successfully to pattern.

7. Click **OK** to dismiss the dialog.

## 17.9.3 Activating and Deactivating Patterns

This section explains how to activate and deactivate patterns.

If you select an active pattern, you have the option to deactivate it. Whereas if you select an inactive pattern, you have the option to activate it.

### 17.9.3.1 Activating Patterns

To activate patterns:

1. Navigate to the **Patterns Search** page, as described in Section 17.5, "Navigating to the Patterns Search Page."

2. In the **Patterns Search** page, enter the search criteria you want and click **Search**. For information, see Section 17.6, "Searching for a Pattern."

3. Select the row for each pattern you want to activate.

4. Press the **Activate** button.

### 17.9.3.2 Deactivating Patterns

You should be extremely careful when disabling patterns. The system does not check to see whether the pattern being disabled is used in any policy.

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).

To deactivate patterns:

1. To deactivate a pattern, from the **Patterns Search** page select the row for each pattern you want to deactivate and press the **Deactivate** button.

2. To deactivate a pattern from the **Pattern Details** page, press the **Deactivate** button.

## 17.9.4 Editing the Pattern

Care should be taken when editing patterns. Potentially, data that is already collected based on that pattern may no longer be usable after the edit.

For example the data would be unusable if you remove one of the attributes and the buckets created in the past for the pattern had taken into account the attribute that is being removed.

To edit the details of a specific pattern:

1. If you are not on the **Pattern Details** page of the pattern you want to edit, follow the instructions in Section 17.7, "Navigating to the Patterns Details Page."

2. To change the pattern name, evaluation priority, and description, edit the appropriate fields in the **Summary** tab of the **Pattern Details** page.

3. To change the status, select from the status you want.

   To change the status of the pattern, see Section 17.9.5, "Changing the Status of the Pattern."

4. Add or change the member types.

   For information, see Section 17.9.6, "Adding or Changing Member Types."

   For information about member types, see Section 17.1.3, "Member Types and Attributes."

5. Change the evaluation priority

   To change the evaluation priority, see Section 17.9.7, "Changing the Evaluation Priority."

6. To add attributes, see Section 17.9.2, "Adding Attributes."

   For information on attributes, see Section 17.1.3, "Member Types and Attributes."

7. To edit attributes, see Section 17.9.8, "Editing Attributes."

8. To delete attributes, see Section 17.9.9, "Deleting Attributes."

9. Click **Apply**.

### 17.9.5 Changing the Status of the Pattern

Active is the default status of the pattern, but you can change the status to one you want.

These are the pattern states:

- Active

  If data must be collected, the pattern must be in the active state.

- Inactive

  If the pattern is complete, but you do not want the pattern to collect data, select **Inactive**.

- Incomplete

  If the pattern has been created, but you are not ready to decide what attributes to choose yet, select **Incomplete**. Data is not collected for this state.

- Invalid

  If you do not want the pattern to be used, select **Invalid**. Data is not collected for this state.

- Deleted

  The pattern has been deleted, but the system must keep this record to maintain data integrity. No autolearning data analysis is performed for a pattern in this state.

> **Note:** It is recommended that you do not use the **Deleted** status. This status may not be available in future releases.

### 17.9.6 Adding or Changing Member Types

You can select more than one member type to add or change.

If you try to select the same members as another pattern, a message appears: "A pattern with the same member configuration already exists. Are you sure you want to create a new pattern? If you answer "yes," you are allowed to create the pattern.

For information on member type, see Section 17.1.3, "Member Types and Attributes."

Follow these steps to add or change member types.

1. If you are not on the **Pattern Details** page of the pattern, follow the instructions in Section 17.7, "Navigating to the Patterns Details Page."

2. In the **Summary** tab, add or change the actor you want to capture data.

   For example, user is the member type if you want to collect information about the user.

### 17.9.7 Changing the Evaluation Priority

Follow these steps to change the evaluation priority.

1. If you are not on the **Pattern Details** page of the pattern, follow the instructions in Section 17.7, "Navigating to the Patterns Details Page."

2. In the **Summary** tab, change the evaluation priority.

### 17.9.8 Editing Attributes

Follow these steps to edit attributes.

1. Click the **Attributes** tab of the **Pattern Details** page.

   If you are not on the Pattern Details page of the pattern you want to edit, follow the instructions in Section 17.8.1, "Viewing Details of a Specific Pattern."

2. In the **Attributes** page, select the attribute you want to edit.

3. Edit the attribute details and click **Save**.

4. Reorder the attributes if you want.

5. Click **Apply**.

### 17.9.9 Deleting Attributes

Care should be taken when deleting attributes.

For example the data would be unusable if you remove one of the attributes and the buckets created in the past for the pattern had taken into account the attribute that is being removed.

Follow these steps to delete attributes.

1. Click the **Attributes** tab of the **Pattern Details** page.

   If you are not on the **Pattern Details** page of the pattern you want to edit, follow the instructions in Section 17.8.1, "Viewing Details of a Specific Pattern."

2. In the **Attributes** page, click the checkbox next to the **Attribute(s)** you want to delete from the pattern.

3. Click **Delete**.

   If you delete an attribute, it is added to the **Add** list and becomes available the next time you select **Attributes**.

## 17.10 Importing and Exporting Patterns

You may want to import and export patterns from other applications. This section explains how to import and export patterns.

### 17.10.1 Importing Patterns

To import patterns:

1. Navigate to the **Patterns Search** page, as described in Section 17.5, "Navigating to the Patterns Search Page."

2. In the **Patterns Search** page, click **Import Pattern**.

3. In the **Pattern Import** dialog, click **Browse** and locate the pattern file you want to import.

4. Click **OK**.

You cannot create your own pattern import files. There is an extension ".zip" that is used when patterns are exported and only files in zip formats can be used. Other files, such as .xml files cannot be imported as patterns import files.

### 17.10.2 Exporting Patterns

To export patterns:

1. Navigate to the **Patterns Search** page, as described in Section 17.5, "Navigating to the Patterns Search Page."

2. In the **Patterns Search** page, enter the search criteria you want and click **Search**. For information, see Section 17.6, "Searching for a Pattern."

3. Select the row for each pattern you want to export.

4. Select **Export Selected** from the **Actions** menu.

5. In the **Export Patterns** dialog, click **Export**.

6. In the **Save** dialog, click **OK**.

## 17.11 Deleting Patterns

If you have an active pattern and it has collected data, you are not allowed to delete the pattern.

Patterns can be deleted only if there is no association with data and rules. A message appears, saying: "There might be pattern data or associated rules using the data and may become out of sync. Are you sure you want to update?"

When multiple patterns are selected for deletion and if some of the patterns are used or linked to other systems, a warning message appears, stating: "The following instances are linked and cannot be deleted. Do you want to delete the other patterns?" If you answer "yes", the unlinked patterns are deleted.

To delete patterns:

1. Navigate to the **Patterns Search** page, as described in Section 17.5, "Navigating to the Patterns Search Page."

2. In the **Patterns Search** page, enter the search criteria you want and click **Search**. For information, see Section 17.6, "Searching for a Pattern."

3. Select the row for each pattern you want to delete and press the **Delete** button.

   If the patterns selected for deletion are not used or linked to a policy, a warning message is shown asking for confirmation. If you answer "yes", those patterns are deleted.

## 17.12 Using Autolearning Data/Profiling Data

After you have configured patterns (created buckets with members and attributes), activated them, and started collecting data, you are ready to use autolearning.

Setting up OAAM to process autolearning data is described in the following subsections.

### 17.12.1 Create a Policy that Uses Autolearning Conditions

Create a policy that uses the autolearning conditions.

For instructions to create a policy, see Section 17.13.1, "Use Case: Challenge Users If Log In Different Time Than Normally."

### 17.12.2 Associate Autolearning Condition with Policy

For the autolearning condition, associate the pattern you created and modify the condition parameters per your requirements.

There are conditions specific to autolearning that use the collected profiling data to perform certain calculations. These conditions are only applicable to autolearning profiling data and cannot be used for other risk analysis.

For information, see Section 17.13.4, "Use Case: User Logs in During a Certain Time of Day More Than X Times."

The rule evaluates the pattern you selected and autolearning processing is performed.

To learn more about autolearning conditions, see Appendix C, "Conditions Reference."

### 17.12.3 Check Session Details

Perform logins/transactions and check the session details to make sure that the policy that was created triggers and data is collected for patterns and buckets.

For information on how to find out whether the pattern is working properly, see Section 17.13.2, "Use Case: Test a Pattern."

## 17.13 Use Cases

This section describes example use cases for autolearning and patterns.

### 17.13.1 Use Case: Challenge Users If Log In Different Time Than Normally

Jeff is a Security Administrator at Dollar Bank. He wants to challenge users with an OTP if they are logging in at a time of day they do not normally come in. To do this he must configure a security policy and associated groups, rules and patterns.

1. Jeff starts with the pattern. He performs a search for patterns that have users as members since his use case focuses on the behavior of users.

   He sees there are two patterns that have users as members. Neither of them has a time range attribute that works for his use case so Jeff must create a new one.

2. Jeff creates a multi-bucket login checkpoint pattern with "user" member type and first evaluation priority. He then adds a time range attribute from 0:00 - 23:00 and a step size of 4. This pattern creates and populates 6 time range buckets as users log in.

3. Jeff searches for the Post-Authentication checkpoint policies already in the system. There are four of them. Since he wants to challenge with an OTP he wants a policy that contains other rules with OTP challenge outcomes.

4. Next Jeff requires a rule to evaluate the bucket memberships. Jeff searches the rules for one that evaluates if a member has fallen into the current bucket less than a specified percentage in the last specified period. He does not find one so he create one using a user in bucket less than % of time condition.

5. Jeff adds the rule to the policy and links the pattern.

6. He then must link action and alert groups. Jeff searches for an action group that contains the challenge OTP action. He finds that there is one already so he links it to the rule.

7. He searches for an alert group by "time" in the alert message text. He finds one alert group that has an alert with the alert text "device has failed to log in

successfully more than 10 times". This alert is not appropriate for his rule so he decides to create a new alert group and alert.

8. Jeff creates a new alert group for his alert. He then adds a new medium alert to the group with the text "User has fallen into this login time bucket less than 5% of the time in the last 3 months".

9. Finally Jeff links the alert group to the rule.

10. He performs log ins to the system to start autolearning.

### 17.13.2 Use Case: Test a Pattern

Jeff a Security Administrator must make sure the pattern he configured in his use (see Section 17.13.1, "Use Case: Challenge Users If Log In Different Time Than Normally") is working properly.

To test the pattern:

1. One morning at 9:30 am he creates a new test user and then performs 7 successful logins.

2. At 3 pm of that day, he performs 3 successful logins.

3. The next day he logs in at 7 pm and is challenged with an OTP.

   This occurs because he has fallen into the 7 pm time bucket less than 5% of the time in the last month.

4. After the policy and pattern have been in the production system for a month he checks to see if the bucketing in the rule evaluation is accurate. Jeff runs a report to find users that triggered the rule by searching for sessions with the alert, "User has fallen into this login time bucket less than 5% of the time in the last 3 months".

5. He then selects a few of them and searches for their bucket memberships for this pattern in the last month.

   In this way Jeff can see the session where the alert was triggered was at a time that fell into a bucket it had not previously fallen into more than 5% of the time in the last month. From that, Jeff confirms that the policy configuration and pattern are functioning as designed.

### 17.13.3 Use Case: Track Off-Hour Access

Jeff is a Security Administrator at Dollar Bank. He wants to track off-hour access by employees based on a standard day shift. To do this, he must create a pattern for behavior-based profiling on time.

The pattern profiles the login times of users into three 8-hour buckets.

**Figure 17–9   Using Buckets to Track Off-Hour Access**
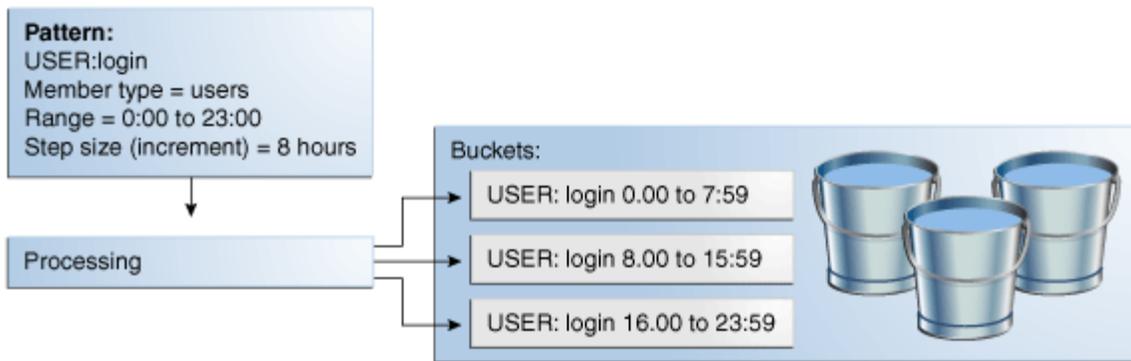


1. Navigate to the **Patterns Search** page, as described in Section 17.5, "Navigating to the Patterns Search Page."

2. In the **Patterns Search** page, click the **New Pattern** button.

3. In the **Create Pattern** dialog, enter the Pattern name: "User: Work hours."

4. Select **Authentication** as the transaction type.

5. From the **Creation Method** list, select **Multi-Bucket**.

6. Select **User** as the **Member Type**.

7. Select **First** as the **Evaluation Priority**.

8. Enter a description.

9. Click **OK**.

   A confirmation is displayed.

10. Click **OK**.

    The **Pattern Details** page appears.

11. Click the **Attributes** tab.

    On this tab you can add/edit the attributes of the users behaviors to be tracked. Choose from available attributes shown in the dropdown list.

12. In the **Attributes** page, click the **Add** button.

13. In the **Add Attributes** dialog, select **Time** from the available attributes shown in the drop-down list.

14. Edit the attribute details.

    a. Select **Active** as the **Status**.

    b. Enter the description.

       For example, "This creates three 8-hour buckets."

    c. Select a compare operator **range** with start value of 0 and end value of 23.

    d. Enter 8 as the Increment Step.

    e. Click **Add**.

15. Click **Apply**.

OAAM creates buckets as needed for the behavior.

### 17.13.4  Use Case: User Logs in During a Certain Time of Day More Than X Times

Jeff is a Security Administrator at Dollar Bank. He wants to be notified with an alert if a user logs in between 10 am to 5 pm more than 3 times. To do this, he must create a pattern that profiles users and time, and an alert group.

1. Create a single bucket pattern called, TimeLog10AM-5PM_PS, with the member type, user.

2. Add the Attribute, Time.

   ■ Compare operator is Range

   ■ Start value is 10 (10 am)

   ■ End value is 17 (5 pm)

3. Create an Alert Group so that an alert is used to notify you about either anomalies or information in the system when rules are triggered.

   For information on Action and Alert groups, see Chapter 12, "Managing Groups."

4. Create a policy that uses autolearning conditions in the Post-Authentication checkpoint.

5. Create a rule within the policy that uses conditions to associate the pattern.

   ■ Ensure that the rule contains the autolearning condition, "Entity: Entity is member of pattern N times."

   ■ Fill in the values for the condition

| Label | Name | Default |
|---|---|---|
| Pattern Hit Count More than | Pattern Hit Count More than | 3 |
| Pattern Name For Membership | Pattern Name for Membership | TimeLog10AM-5PM_PS |
| is Membership Count more than the Pattern Hit Count for User | isMoreThan | true |
| Time period type for pattern membership | Time Period Type for Patternmembership | hours |
| Time Period Type for Pattern Membership | Time Period Type for Pattern Membership | 1 |
| Member Type for pattern Membership | MemberType for pattern Membership | user |

   ■ Add the Alert group as a result of the rule.

6. Group link to user group.

7. Verify that the alerts are generated, starting with the fourth login.

### 17.13.5  Use Case: Patterns Can have Multiple Member Types

Jeff is a Security Administrator at Dollar Bank. He wants to track logins by employees based on days of the week and devices. To do this, he must create a pattern to profile the days of the week, users, and devices login.

If Joe logs in on Monday, his User ID and the Device ID of the computer he is using are added to the Monday bucket once. If Fred uses the same computer to log in on

Monday, his User ID and the Device ID of the computer will be added once. At that point, the Monday bucket will have one count for Joe, one count for Fred, and two counts for the device. Rule conditions are then used to evaluate the bucket memberships.

A rule could be created to evaluate one member type of multiple member types.

For example,

- Joe logged in on Tuesday less than 5% of the time in the last two months

- Joe and this computer logged in on Tuesday less than 5% of the time in the last two months

To set up patterns so that they can have multiple member types with the members independently profiled by the pattern, you perform the following steps.

1. Create a pattern with User and Device as entities. It will have "Day of the Week" as the attribute and the operator for the attribute will be "for each."

   Describe the bucket population correctly.

   The condition to use is "Entity member of pattern (fingerprint) less than percentage times (as compared to its own data)."

   For information, see Section C.2.1.2, "Pattern (Authentication): Entity is Member of Pattern Less Than Some Percent Time."

2. Create one rule.

   a. Set the percent value to be 5% in the rule.

   b. Set the pattern described in Step1 as the pattern in the rule.

   c. Set the entity to be user.

   d. Set time period to 2.

   e. Set time period type to months.

   f. Leave the other values to the default.

3. Create another rule.

   a. Set the percent value to be 5% in the rule.

   b. Set the pattern described in Step1 as the pattern in the rule.

   c. Set entity to be device this time.

   d. Set time period to 2.

   e. Set time period type to months.

   f. Leave the other values to the default.

### 17.13.6 Use Case: City Usage

Joe's company wants all users to be challenged with an OTP if they are logging in from a city they are not a member of.

Joe logs in from three cities (home, office A and office B). A city pattern records how often he logs in from each.

| Bucket | Location |
|---|---|
| City Bucket #1 | home |

| Bucket | Location |
|--------|----------|
| City Bucket #2 | office A |
| City Bucket #3 | office B |

Joe's company wants users to be challenged with an OTP two sessions in a row if they are logging in from a city they have not used in the last month. If Joe stops working at office B for 37 days and does not access from anywhere else in that city he will be challenged for an OTP the next time he logs in from that city. To accomplish this use case a rule will be configured to check on the membership count for the current city bucket in the last month. The count threshold will be set to two so the rule will trigger until the user has been a member at least twice in the last rolling month window.

To set up the system so that users are challenged with an OTP if they are logging in from a city they are not a member of, perform the following steps.

1. Create a pattern with **User** as the actor, **City** as the attribute, and **For Each** as the compare operator.

2. Use the condition, "Entity is member of bucket less than N times in given time period"

3. Set the rule parameters for conditions as:

   a. **Pattern Name** as the pattern that you have created.

   b. **Time period type** is **month**.

   c. **Time period** is **1**.

   d. **Count** is **3**.

   e. Operator if required is **less than**.

The rule will trigger (and challenge) the user, if the user has not used that city more than 2 times in the last month (in last 30 days).

## 17.13.7  Use Case: Autolearning Adapts to Behavior of Entities

In addition to profiling, collecting data, and checking it, autolearning adjusts so that the system acts depending on the user's behavior. Conditions and the specified percentage remain unchanged.

If you log into the bank application from California everyday, but then you locate to Seattle without informing your bank. When you log in for the first time from Seattle, you are challenged. The second time, you are challenged again because you are logging in from a city less than 50% of your total logins within 1 month. The system knows Seattle is not the usual place you log in from. You are annoyed, but do not consider it a hindrance yet. Challenging you again will degrade your user experience.

The condition, therefore, has to be configured in such a way that there is a percentage when the system knows that it should no longer challenge you. The system should automatically be smart enough to understand that you are logging in from Seattle every time now going forward and that it should not challenge you.

The system does not challenge you when you log in a third time from Seattle. When you fly to California after three months the system challenges you when you log in. The system wanted to make sure that you are the person logging in to the system.

**Example**

You want the system to KBA challenge the user if the user logs in from a city less than 50% of the time within a month.

1. Create a multi- bucket pattern for each city called, UserLoginsCity.

   - Member type is user

   - Attribute is City; compare operator is "for each"

   When a user logs in from different cities a bucket will be created for each city

2. Create an Action Group to KBA challenge the user for each city less than % membership.

3. Create policy that will use autolearning conditions in the Post-Authentication checkpoint.

4. Create a rule within the policy that uses conditions to associate the pattern.

   The rule will calculate the percentage membership of a user belonging to a pattern

   - Ensure that the rule contains the autolearning condition, "Entity: Entity is member of pattern less than some percent times".

     For information on this condition, see "Pattern (Authentication): Entity is Member of Pattern Less Than Some Percent Time".

   - Fill in the values for the condition

| Label | Default |
|---|---|
| Pattern Hit Percent less than | 50 |
| Pattern name for membership | UserLoginsCity |
| Is Membership Count Less than patternHitPercent | True |
| Time period type for pattern membership | Month |
| Time period for pattern membership | 1 |
| Member type for pattern membership | User |

   - Add the Action group as a result of the rule.

5. Group link to user group.

6. If the user logs in from a city < than 50% of the total logins within 1 month, the user is challenged.

## 17.13.8  Use Case: Single Bucket Pattern

Single-bucket (manually created) patterns create and populate one bucket with the exact data points and value ranges specified in the pattern. You can create a pattern that describes behavior that has been deemed to be high risk based on industry expertise.

You can configure a bucket so that OAAM can look for any traffic that falls in:

- 8am -10am pattern

- New location

- New device

- New transfer account, not owned by this user is created

- Wire transfer to new account

This specific combination has been known to be a very high fraud risk in the past so you want to challenge with an OTP through SMS any time this pattern is seen.

## 17.13.9 Use Case: Using Pattern

A Security Administrator must configure a policy that challenges a user with a challenge question if the user is logging in from a state that he or she does not log in from very often, specifically one that he or she uses less than twice in a month.

The outcome should include a score and an alert.

### Why use patterns for this scenario

This evaluation involves both profiling (patterns) and the rules to evaluate those patterns.

Patterns are used in this scenario for the following reasons:

- If rules are to track the frequency of behavior, the period for evaluating the frequency might be relatively long, especially if the evaluation requires months or even years. Using a pattern is recommended in these cases because rules will not have to perform large queries for results. Oracle Adaptive Access Manager checks the bucketing to see if the user is a member of the current state bucket that he is falling into now and the frequency at which he has fallen into that bucket.

- Other rules that run can use the pattern, which tracks the state or frequency of state usage, for other types of risk evaluations. By using the same pattern, no overhead is incurred to impact performance.

### Steps

1. Log in to OAAM Admin as an administrator.

2. In the Navigation tree, double-click **Patterns**. The **Patterns Search** page is displayed.

3. Click the **New Pattern** button.

   Create a pattern where:

   - **Creation Method**: Multi-bucket

   - **Member Type**: User

   - E**valuation Priority**: High

   - **Description**: Pattern to track the state usage and frequency

   Click **Create**.

4. Click the **Attribute** tab.

5. Click the **Add** button.

6. In the **Add Attribute** dialog, select **State** as the attribute and click **Next**.

7. In the page following, select **for Each** as the **Compare Operator** and click **Add** and then **OK**.

   The compare operator **for Each** is selected to profile every state that users log in from (a bucket is created for each state and populated with users as they fall into the buckets).

8. In the Navigator tree, double-click **Group**.

9. Click **New Group**. The **Create Group** dialog is displayed.

10. Create a new `StateNotUsedOften` alert group.

   - **Group name**: State not used often

   - **Group type**: alerts

   - **Caching policy**: Full cache since the group is used in rules and conditions.

11. Click **Create** and then **OK**. The **Group Details** page is display.

12. In the **Alerts** tab of the **Group Details** page, click **Add Member**.

13. In the **Add Member** page, select **Create new element**.

14. Select the **Customer Care** as the alert type.

15. Select the **Medium** as the alert level.

16. Type in the alert message in the **Alert Message** box.

   For example, user is logging in from a state he or she has used less than 2 times in a month.

17. Click **Add** to create and add the new alert to the alert group.

18. When the confirmation dialog appears, click **OK** to dismiss the dialog.

19. In the Navigation tree, double-click **Policies**. The **Policies Search** page is displayed.

20. Search policies for post-authentication policies that are available.

   In best practices, KBA challenges occur in the Post-Authentication checkpoint.

   Because the rule being created will have the outcome of a KBA challenge, it will have to be in the Post-Authentication checkpoint. It must also be in a policy in which there is a check for KBA registration before this rule runs.

21. Open the policy to the details page and click the **Rules** tab.

22. Click **Add**.

23. Plan the rule:

   A rule should be created to KBA-challenge the user if it is triggered; therefore the rule must be contained in a policy with other rule challenges.

   Because the rule will result in a KBA challenge, the best practice is for the scoring that you set and configure for the rule to have a relationship to the action/outcome of that rule and to the severity of that rule that is being evaluated. The severity of the situation, the action for which the rule would trigger, and the score in which the rule would generate must be proportional to each other.

   The rule is checking if the user is logging in from a state that he has logged in from recently, but the situation does not necessarily mean fraud. The situation is one of medium risk--that is why a KBA challenge is used instead of a block. A KBA challenge is appropriate for the scores in the 500 to 700 risk range. For this example, a score of 600 is specified. An OTP challenge would have been appropriate for a score in the 701 to 900 range. For a score of 900 and over, the action triggered should be a "block." The user should be allowed to continue on if the score is under 500.

24. Enter the summary information and click the **Results** tab.

25. Enter `600` as the score.

**26.** Enter 100 as the weight.

**27.** Select **ChallengeQuestionPad** as the action.

**28.** Select **StateNotUsedOften** as the alert.

**29.** Click the **Conditions** tab.

**30.** Click **Add** and select Pattern (Authentication): Entity is Member of Pattern N Times.

Enter the following values:

| Label | Name | Default |
| --- | --- | --- |
| Pattern Hit Count More than | Pattern Hit Count More than | 2 |
| Pattern Name For MemberShip | Pattern Name for MemberShip | user:state |
| is MemberShip Count more than the Pattern Hit Count for User | isMoreThan | false |
| Time period type for pattern membership | Time Period Type for Patternmembership | month |
| Time Period Type for Pattern MemberShip | Time Period Type for Pattern MemberShip | 1 |
| MemberType for pattern Membership | MemberType for pattern Membership | user |

**31.** Click **Save** to save your changes.

A confirmation dialog displays the status of the operation.

**32.** Click **OK** to dismiss the confirmation dialog.

## 17.13.10 Use Case: Logins from Out of State

Acme is a small business group and all their clients are local to the city and are not expected to travel out of the state very often. The business group wants to track all logins occurring from other states, so they can challenge the users and also trigger a high alert so they can investigate to ensure that it is a valid user logging in from the other state. If they are valid, they will be added to an "Allow User group" so they will not be challenged the next time they log in from another state.

**1.** Set autolearning properties to true.

- vcrypt.tracker.autolearning.use.auth.status.for.analysis
- vcrypt.tracker.autolearnin.enabled

**2.** Create a single bucket pattern with the following parameters so the pattern tracks all logins not occurring from this state. Essentially the counter will be incremented every time the login occurs from another state.

- Transaction Type: Authentication
- Attribute: State
- Compare Operator: Not in
- Compare Value: State name
- Member Type: User

■ Evaluation Priority: First

3. Use this pattern in a rule condition.

    a. Create a rule.

    b. Add the condition, ENTITY: Entity is member of pattern N times.

       – Pattern hit count more than: count

       – Pattern Name for membership: Pattern name

       – Is Membership Count More than patternHitCountForUser: True

       – Time period type for pattern membership-- Hours

       – Time period for pattern membership: 1

       – Member type for pattern membership-- User

4. Save the policy and rule.

5. Simulate a few logins from different states. The users should be challenged and a high alert should be triggered.

6. Add a user to the "White User Group".

7. Add this user group to  "excluded user group" in the pre-conditions in the rule.

8. Save the policy and rule.

9. Repeat step 5. Users in the White User Group will not be challenged.

## 17.14  Autolearning Properties

Autolearning properties and their default values out of the box are listed in this section.

| Property | Default Value | Property Type | Is Dynamic | Comments |
|---|---|---|---|---|
| vcrypt.bharosa.autolearning.numPriorities | 2 | Integer | No | This creates the number of threadpools as the number of priorities. These threadpools are used for post processing the autolearning data. This number should be more than 1. |
| vcrypt.bharosa.autolearning.threadMultiplier | 7 | Integer | No | This number is used to create the number of threads for post processing. These threads are part of the threadpool that is used for post processing autolearning data. Keep this number to at least 5. |

| Property | Default Value | Property Type | Is Dynamic | Comments |
|---|---|---|---|---|
| vcrypt.tracker.autolearnin.enabled | true | Boolean | Yes | This flag is used to control the status for the product level. Setting the value to false disables some of the post processing for autolearning. Rules continue to run but may be using stale data. |
| vcrypt.tracker.autolearning.use.auth.status.for.analysis | false | Boolean | Yes | This flag is used when the client code does not explicitly call the autolearning API. If you want autolearning (post processing) to occur but do not want to change the client code, setting this flag to true results in autolearning processing for the authentication type of updateAuthStatus requests if the status is SUCCESS for that authentication request. However if the status is not SUCCESS, autolearning does not occur. Running autolearning rules with this flag set to false runs the rules on the data that is stale. If this flag is set to false and autolearning rules are running, and if the log level is set to "debug" for "com.bharosa.vcrypt.tracker.rules.impl.VCryptTrackerAutoLearningImpl" class; then a message is written to the log saying that this property is disabled and rules are still being run. |

| Property | Default Value | Property Type | Is Dynamic | Comments |
|---|---|---|---|---|
| vcrypt.tracker.autolearning.use.synchronous.execution.for.pattern.analysis | false | Boolean | Yes | This property controls whether the pattern analysis occur in synchronous mode. If set to true, pattern analysis is performed in synchronous fashion. The updateAuthStatus or updateTransactionStatus call may take longer to complete since all the pattern data update occurs as part of the same updateStatus call. |
| vcrypt.tracker.autolearning.update.entity.profile.for.auth.patterns | true | Boolean | Yes | If this property is set to false, profiles for entities are not updated as part of pattern analysis. |
| bharosa.menu.queries.entities | false | Boolean | Yes | This flag determines whether the menu item to view historical data should be shown in the OAAM Admin Console. |
| bharosa.arm.pagetitle.queries.entities.patternworkflow | | String | Yes | Default location of the menu for the pattern historical data. Use this historical data page to check if pattern data collection is functioning properly. |

## 17.15 Checking if Autolearning Pattern Analysis Functioning

To quickly find out if Autolearning is functioning, perform the following steps:

1.  Ensure that the base authentication-related entities are installed and that the following properties are set to true.

    -   vcrypt.tracker.autolearnin.enabled

    -   vcrypt.tracker.autolearning.use.auth.status.for.analysis

2.  Make sure that patterns are defined and active. You should have at least one pattern that has **User** as a member type and **time**, **city**, **state**, or **country** as an attribute. For time choose **Range** as the operator. If you choose the other attributes, choose **For Each** as the operator. You should choose only one attribute so that you can use this pattern as a test pattern.

3.  Log in to the OAAM Server a few times.

4.  Perform the following database queries on the v_fprints table.

    Run

"select * from v_fprints where pattern_id is not null and
create_time > sysdate - 1/96"

This will return pattern based fingerprints created in last 15 minutes.

Run

"select * from vt_wf_days where fprint_id in (select
fprint_id from v_fprints where pattern_id is not null and
create_time > sysdate - 1/96) "

If this returns records and the record shows a positive integer in "today's day
column", autolearning is working. Note: If today is the 15th then look into the
Day_15 column in the records returned by this database query.

## 17.16 Checking if Autolearning Rules are Functioning

To check if the rule were triggered, create a time based pattern that tracks the user.

1. Create a policy (post authentication) and add the User first time bucket rule to it.
   Select the time based pattern and leave all other values to default.

2. Save the policy.

3. Perform logins from the authenticator using new user names.

   If autolearning processing worked then the rule added to the above policy should
   trigger.

4. After this perform the same logins again in the same hour.

   If autolearning rule is working the rules should not trigger for this second login.

## 17.17 Autolearning Classes and Logging

Important classes for logging to debug level is summarized below.

*Table 17–2   Autolearning Classes and Logging*

| Class Name/Logger | What does debug logging do |
| --- | --- |
| com.bharosa.vcrypt.tracker.autolearning.VCryptAuthPatternAnalysisRequest AND com.bharosa.vcrypt.tracker.autolearning.VCryptTransactionPatternAnalysisRequest | Prints debug log when processing the request. Time required to process the autolearning request is printed as milliseconds. All function entry and exit points are logged along with incoming and outgoing parameters |
| com.bharosa.vcrypt.tracker.rules.impl.VCryptTrackerAutoLearningImpl | Prints debug log when processing autolearning rules. Request ID is printed along the log statements so you can track the log with the session. All function entry and exit points are logged along with incoming and outgoing parameters |
| com.bharosa.vcrypt.tracker.autolearning.VCryptAutoLearningRulesUtil | This class implements most of the logic in autolearning rules. Request ID is printed along the log statements so you can track the log with the session. All database queries are also printed. The time required to database query is available from the time in log statements. All function entry and exit points are logged along with incoming and outgoing parameters |

## 17.18 Pattern Attributes Reference

Information about the pattern attributes is presented in this section.

*Table 17–3    Pattern Attributes*

| Name | Description | Type | Operators | Valid Values | Buckets | Comments (Applicable Rules) |
|------|-------------|------|-----------|--------------|---------|------------------------------|
| dayOfMonth | Day Of the Month (First day = 1, Last Day will vary) | Integer | Equal, not equal, For Each, Less than, Less than Equal to, greater than, greater than equal to, in, not in, range | 1 through 31 | multi-bucket | User - themselves and all |
| monthOfTheYear | Month Of the Year (January = 0, December = 11) | Integer | Equal, Not Equal, For Each, Less than, Less than Equal to, greater than, greater than equal to, in, not in, range | 0 through 11 | multi-bucket | User - themselves and all |
| Connection Type | Connection Type for the authentication request. The value for this attribute is a positive integer number that indicates the connection type. Examples of connection type are optical connection, wireless connection, dialup connection, T1/T3 type of connection, DSL connection, cable connection, and so on. Refer to location.connection.type.enum for more information on connection type. | Integer | Equal, Not Equal, For Each, Less than, Less than Equal to, greater than, greater than equal to, in, not in, range | lookup location.connection.type.enum | multi-bucket | ▪ User - themselves<br>▪ Device - themselves and all<br>▪ Location - themselves |
| Connection Speed | Connection Speed for the authentication request. The value for this attribute is a positive integer number that indicates the connection speed. Examples of connection speed are High, Medium, Low, and so on. Refer to connection.linespeed.enum for more information. | Integer | Equal, Not Equal, For Each, Less than, Less than Equal to, greater than, greater than equal to, in, not in, range | lookup connection.linespeed.enum | multi-bucket only | ▪ User - themselves<br>▪ Device - themselves and all |
| Routing Type | Connection routing type for the authentication request. The value for this attribute is a positive integer number that indicates the routing type. Examples of routing type are POP, Proxy, AOL, and so on. More information on routing type can be found in location.routing.type.enum. | Integer | Equal, not equal, for each, less than, less than equal to, greater than, greater than equal to, in, not in, range | lookup location.routing.type.enum | multi-bucket only | ▪ User - themselves and all<br>▪ Device - themselves and all |

*Table 17–3   (Cont.)  Pattern Attributes*

| Name | Description | Type | Operators | Valid Values | Buckets | Comments (Applicable Rules) |
|------|-------------|------|-----------|--------------|---------|------------------------------|
| Browser | Browser used for the authentication request. Examples of browser are Mozilla, Opera, and so on. | String | For each, in, not in, like, not like | Any string value | multi-bucket only (rarely single) | ■ User - themselves and all<br>■ Device - themselves and all |
| Operating System | Operating System used for the authentication request. Examples of Operating System are Unix, Linux, Windows, and others. | String | For each, in, not in, like, not like | Any string value | multi-bucket | ■ User - themselves and all<br>■ Device - themselves and all |
| locale | Locale used for the authentication request. Examples of Locale are en_US, fr_CN, en_GB, and so on. | String | For each, in, not in, like, not like | Any string value | multi-bucket only | ■ User - themselves and all<br>■ Device - themselves and all<br>■ IP - themselves and all |
| Device Fingerprint Identifier | Device Fingerprint Identifier available for the authentication request. This number is calculated depending on the device used by the user for this authentication request. | Long | For each, equals, less than, less than equal to, greater than, greater than equal to, in, not in, not equal, range | Any positive number (java.lang.Long) | multi-bucket | ■ User - themselves<br>■ Device - themselves |
| Cookie Enabled Status | This boolean variable tracks if the cookie was enabled or disabled on the user's device/browser for this authentication request. | Boolean | For each, not equal, equal | True or False | multi-bucket | User - themselves |
| Cookie Status | This variable tracks the status of the device/browser cookie. This is a positive integer that corresponds to status of the browser cookie. Examples of the status are Learn mode (0), Enabled (1) and Disabled (2), and so on. More information on cookie state can be found in cookie.state.enum. | Integer | Equal, not equal, for each, less than, less than equal to, greater than, greater than equal to, in, not in, range | lookup cookie.state.enum | multi-bucket | User - themselves |
| Screen Resolution (based on flash) | This variable tracks the screen resolution used by the user.This attribute is usually available in the form of MxN (M by N) pixels. One of the example is 1600x1200 (pixels). | String | For each, in, not in, like, not like | Any string value. Usually the resolution will appear like MxN. e.g.(1600x1200) | multi-bucket only | Device - themselves |

*Table 17–3   (Cont.)  Pattern Attributes*

| Name | Description | Type | Operators | Valid Values | Buckets | Comments (Applicable Rules) |
|------|-------------|------|-----------|--------------|---------|------------------------------|
| Color screen (based on flash) | This variable tracks whether the user's device has color screen. | Boolean | For each, not equal, equal | True or False | multi-bucket | Device - themselves |
| Audio encoder (based on flash) | This variable tracks whether the user's device has audio encoder. | Boolean | For each, not equal, equal | True or False | multi-bucket | Device - themselves |
| Accessibility (based on flash) | This variable tracks whether the user's device has accessibility provisions. | Boolean | For each, not equal, equal | True or False | multi-bucket | User - themselves |
| Has audio (based on flash) | This variable tracks whether the user's device has audio capabilities. | Boolean | For each, not equal, equal | True or False | multi-bucket | Device - themselves |
| Country | Country | String | For each, in, not in, like, not like | Any string value | single and multi-bucket | <ul><li>User - themselves and all</li><li>Device - themselves and all</li></ul> |
| State | State | String | For each, in, not in, like, not like | Any string value | single and multi-bucket | <ul><li>User - themselves and all</li><li>Device - themselves and all</li></ul> |
| City | City | String | For each, in, not in, like, not like | Any string value | single and multi-bucket | <ul><li>User - themselves and all</li><li>Device - themselves and all</li></ul> |
| Time | Time when the user is logged in | Integer | Equal, Not Equal, For Each, Less than, Less than Equal to, greater than, greater than equal to, in, not in, range | Integer values (0-23) | multi-bucket | User - themselves and all |
| Day of Week | Day of the week (Sunday = 1, Saturday = 7) | Integer | Equal, Not Equal, For Each, Less than, Less than Equal to, greater than, greater than equal to, in, not in, range | Integer (1-7) | single and multi-bucket | User - themselves and all |

*Table 17–3   (Cont.)  Pattern Attributes*

| Name | Description | Type | Operators | Valid Values | Buckets | Comments (Applicable Rules) |
|------|-------------|------|-----------|--------------|---------|-----------------------------|
| 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. | Integer | Equal, Not Equal, For Each, Less than, Less than Equal to, greater than, greater than equal to, in, not in, range | Positive integer value | multi-bucket | ▪ User - themselves and all<br>▪ Device - themselves and all<br>▪ Location - themselves and all |
| User ID | User's Identification Number | String | For each, in, not in, like, not like | String value | multi-bucket | ▪ Device - themselves<br>▪ Location - themselves |
| Group ID | Group Identification Number | String | For each, in, not in, like, not like | any String value | multi-bucket | ▪ Device - themselves<br>▪ Location - themselves |
| Device ID | Device Identification Number | Integer | Equal, Not Equal, For Each, Less than, Less than Equal to, greater than, greater than equal to, in, not in, range | any String value | multi-bucket | ▪ User - themselves<br>▪ Location - themselves |

*Table 17–3    (Cont.)  Pattern Attributes*

| Name | Description | Type | Operators | Valid Values | Buckets | Comments (Applicable Rules) |
|------|-------------|------|-----------|--------------|---------|------------------------------|
| Remote 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. | String | For each, in, not in, like, not like | format a.b.c.d | multi-bucket | <ul><li>User - themselves</li><li>Device - themselves</li></ul> |
| 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. | Boolean | For each, not equal, equal | True or False | multi-bucket | User - themselves |
| ISP | The ID for an Internet connection service provider. | Long | For each, equals, less than, less than equal to, greater than, greater than equal to, in, not in, not equal, range | Any positive number | multi-bucket | <ul><li>User - themselves and all</li><li>Device - themselves and all</li></ul> |

## 17.19  Pattern Attributes Operators Reference

Information about the pattern attribute operators is presented in this section.

The **Day of Week** and **City** attributes are used in the examples that follow to illustrate how operators work.

Numbers corresponding to the days of the week are:

- 1 = Sunday
- 2 = Monday
- 3 = Tuesday
- 4 = Wednesday
- 5 = Thursday
- 6 = Friday
- 7 = Saturday

Oracle Adaptive Access Manager will create buckets dynamically as necessary. The first time the criteria specified is fulfilled, Oracle Adaptive Access Manager will create a bucket for the criteria and add the actor as a member with a count of one. The next time the criteria is fulfilled, the actor is added to that same bucket as a member with a count of one. Each subsequent time the criteria is fulfilled, the bucket counter will be incremented.

### 17.19.1 For Each

If the **For each** attribute is set, a bucket is created for each distinct value of the attribute.

When the user specifies For Each, and **Day of Week** as the attribute, a bucket will be created dynamically for each day of the week as required and the counts updated for the buckets as logins occur.

### 17.19.2 Equals

If the **Equals** operator is set, the bucket is created and then the count updated only when the attribute value equals the value specified in the Compare Value field.

When the user specifies **Day of Week** as the attribute and enters 7 (Saturday) in the Compare Value field, a bucket is created for Saturday and the count updated as soon as he logs in on Saturday. The other days do not fulfill the criteria he specified.

### 17.19.3 Less Than

If the **Less Than** operator is specified, a bucket is created and the count updated only when the attribute value is less than the value specified in the Compare Value field.

When the user specifies **Day of Week** as the attribute and enters 4 (Wednesday), a single bucket is created for Sunday (day=1), Monday (day=2), and Tuesday (day=3) and all his logins on Sunday, Monday, and Tuesday will be counted as part of that bucket.

### 17.19.4 Greater Than

If the **Greater Than** operator is specified, a bucket is created and the count updated only when the attribute value is greater than the value specified in the Compare Value field.

If the user specifies **Day of Week** as the attribute and enters 3 (Tuesday), a single bucket is created and the count updated only for Wednesday (day=4), Thursday (day=5), Friday (day=6), and Saturday (day=7). A bucket will not be created nor will the count be updated for the user for Tuesday (day=3).

### 17.19.5 Less Than Equal To

If the **Less Than Equal To** operator is specified, a bucket is created and the count updated only if the attribute value is less than or equal to the value specified in the Compare Value field.

When the user specifies Day of Week as the attribute and enters 3 (Tuesday), a bucket will be created and the count updated when the user logs in on Sunday (day=1), Monday (day=2), and Tuesday (day=3). In Less Than Equal To 3, Tuesday (day=3) also qualifies as meeting the bucket population criteria.

### 17.19.6 Greater Than Equal To

If the **Greater Than Equal To** operator is specified, a bucket is created and the count updated only if the attribute value is greater than or equal to the value specified in the Compare Value field.

When the user specifies Day of Week as the attribute and entered 3 (Tuesday), a bucket will be created and the count updated when the user logs in on Tuesday (day=3), Wednesday (day=4), Thursday (day=5), Friday (day=6), and Saturday (day=7). In

Greater Than Equal To 3, Tuesday also qualifies as meeting the bucket population criteria.

### 17.19.7 Not Equal

If the **Not Equal** operator is set, a bucket is created and the count updated when the authentication/transaction attribute has a value not equal to the value specified in the Compare Value field by the user.

In the Day of Week example, if the user specifies a value of 1 (Sunday), a single bucket will be created for all logins other than Sunday (day=1).

### 17.19.8 In

The **In** operator works like the **Equals** operator except all the comma separated values in the Compare Value field are used for an "equals to" comparison. In the Day of Week example, if the user enters 1,2,3,4,5, a single bucket is created for all logins that fall on Sunday (day = 1) through Thursday (day =5).

### 17.19.9 Not In

The **Not In** operator works exactly the opposite of **In**. In the Day of Week example, if the user enters the values 1,2,3,4,5 for the day of the week, a single bucket is created for Friday (day = 6) and Saturday (day =7) only.

### 17.19.10 Like

The **Like** operator is applicable and enabled only for string type attributes. If the user's login "city" is used as the attributes and he specifies "San" for the city attribute, his logins from the cities, "San Francisco," "Santa Clara," "San Jose," and "Sangamner" will result in a single bucket and updates to the count.

"Like" compares the string attribute's value with the one specified by the user.

### 17.19.11 Not Like

The **Not like** operator is applicable and enabled only for string type attributes. If the user's login "city" is used as the attribute and he specifies "San" for the **City** attribute, his logins from the cities, "San Francisco," "Santa Clara," "San Jose," and "Sangamner" will not result in the creation of a bucket or updates to the count. His logins from Redwood City, Austin, and other cities that do not have "San" in the name will result in a single bucket and updates for this pattern.

### 17.19.12 Range

**Range** is usually used with numerics.

*Figure 17–10   Range Compare Operator*



### 17.19.12.1  Fixed Range

When the user enters values for **Start Value** and **End Value** and leaves the **Increment Step** value as 0, he wants to create a bucket for the activity when the attribute value is **Greater Than Equal To** the **Start Value** and **Less Than Equal To** the **End Value**. Using the Day of Week example, if the user enters 1 (Sunday) as the **Start Value** and 5 (Thursday) as the **End Value**, all the logins from Sunday (day=1) through Thursday (day=5) will result in the creation and updates to the count of a single bucket. A fixed range is when the upper and lower limit are fixed and there are no steps "in between" (the increment step is not entered by user).

### 17.19.12.2  Fixed Range with Steps (or Increment)

When the user enters values for **Start Value** and **End Value** and also provides a value for the **Increment Step**, he wants to create a bucket for the activity when the attribute value is **Greater Than or equal** to the **Start Value** and **Less Than Equal To** the **End Value** and he wants to create finer level buckets which are separated by the "increment" value of the attribute. Using the Day of Week example, if the user enters 1 (Sunday) as the **Start Value** and 5 (Thursday) as the **End Value** and the **Increment Step** as 1, all the logins from Sunday (day=1) through Thursday (day=5) will result in the creation and updates to the count of multiple buckets. A bucket will be created and updated for the day starting Monday and then for each day (since the increment is one).

### 17.19.12.3  Upper Unbound Ranges with Steps

Upper unbounded ranges with increment steps are used for items, such as numbers, such as amounts. Basically, multiple-tiered ranges can be configured.

For example you can configure

0 to 100 with Step 10.

101 to 1000 with Step 100.

1001 to 10000 with Step 1000.

10001 to ...  with Step 10000.

All the ranges but the last one works the same way as the earlier range example with **Start Value** and **End Value** with **Increment Step**.

The last range works as if the upper limit is infinity. In this scenario, buckets are created for each 10000 (ten thousand) after 10001 (ten thousand one).

If a user has an amount of 200,123 (two hundred thousand 123), a bucket would be created for him for 200,000 through 210,000. His transaction for this amount will fall into this bucket.

# 18

# Managing Configurable Actions

Oracle Adaptive Access Manager provides many standard actions that are handled by a web application. These standard actions include block, KBA challenge, password TextPad, and others. The standard actions can also be used as trigger actions for **Configurable Actions**. Configurable actions are external Java code that is triggered by OAAM Server. Customers can write any java code they wish to perform custom operations without any change to Oracle Adaptive Access Manager. The Configurable Actions feature allows for endless customizations.

This chapter provides an overview on configuring a configurable action and instructions on how to define, view, edit, and delete an action instance, and on how to associate action instances to a **Checkpoint**.

## 18.1 Introduction and Concepts

This section introduces you to the concept of configurable actions and how they are used in Oracle Adaptive Access Manager.

### 18.1.1 Configurable Actions

Configurable actions are actions that are triggered based on the result action or risk scoring or both after a checkpoint execution.

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

An example of a configurable action is an email that is sent to you whenever a checkpoint execution returns "block" as an action in the result. In this case, "Send Email" is the configurable action and "block" is the trigger criteria. Similarly, there could be configurable actions that can be based on a "risk score" as the trigger criteria.

Java classes and action templates for certain configurable actions are provided out-of-the-box, but you have the option to create configurable actions based on your needs. For detailed steps on configuring the default configurable actions, see Section 18.20, "Out-of-the-Box Configurable Actions."

### 18.1.2 Action Templates

Action Templates let you define the common details of the configurable action. You can specify the java class that is tied to the action and also specify default parameter values of the action.

The configurable actions are built using action templates. You can create only one action template per Java class file. You can create custom Java class files and corresponding action templates for your needs.

For example, if you had an action template, "add to a group," you could create four instances of the action template:

- Add user to a white-list group

- Add user to black-list group

- Add IP to IP white-list group

- Add IP to IP black-list group

Using the action template, you create an action instance based on your scenario. For example, you could have an instance such as "create a case whenever there is a block action" or another instance such as "create a case whenever there is a challenge action."

### 18.1.3 Deploying a Configurable Action

A flow chart illustrating the deployment of a Configuration Action is shown in Figure 18–1.

**Figure 18–1    Develop and Deploy a Custom Configuration Action**
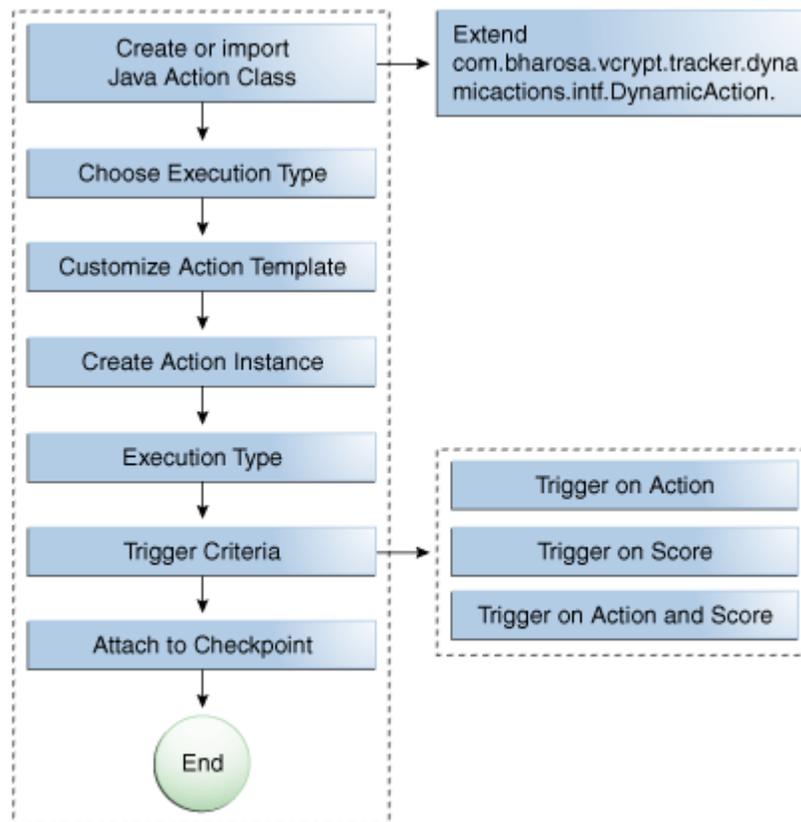


> **Note:**   Steps to install newly created java class are included in this illustration.

The chapter has been organized into sections by topic. If you have configured configurable actions before, use this chapter as a reference.

If you want configurable actions enabled in your system, follow this process:

1. Enable the configurable action property.

   Set `dynamicactions.enabled` to `true`.

2. Make sure the configurable action definitions are configured in the Oracle Adaptive Access Manager database.

   Out-of-the-box configurable action templates are imported when you import the snapshot when you are setting up OAAM's base environment.

   A user can see the list of available configurable actions before adding a new one.

3. Determine what configurable actions have to be added to which checkpoint and the preconditions for executing those configurable actions.

4. If the existing Configuration Actions are not sufficient, develop and deploy custom ones. See the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager* for details on developing a configurable action.

   Although some configurable actions are provided with the product, you may have to develop custom templates for your particular requirements.

   a. Define the custom action template

   b. Load the action template

5. Associate the configurable actions to the Checkpoint.

## 18.2 Creating Configurable Actions

The configurable action creation flow is presented in this section.

You can:

- Use an existing action template or create a new one to create a configurable action.

- Define an action instance/create a configurable action

*Figure 18–2   Configurable Action wizard Flow*
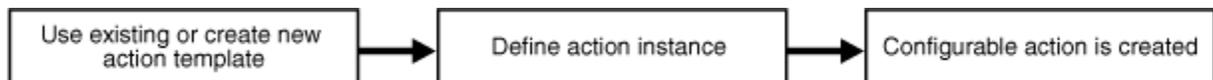


### 18.2.1 Define New Action Template

If you want to define a new action template, see Section 18.6, "Creating a New Action Template" for detailed information.

### 18.2.2 Use Existing Action Template

If you want to use an existing action template, see Section 18.4, "Searching for Action Templates."

### 18.2.3 Create Action Instance

To define an action instance, see Section 18.9, "Creating an Action Instance and Adding it to a Checkpoint" for detailed information.

## 18.3 Navigating to the Action Templates Search Page

You manage action templates in Oracle Adaptive Access Manager from the Action Templates Search page. From this page, you can search, view, create, export, and delete action templates.

1. In the Navigation tree, expand **Configurable Actions**.

2. Click **Action Templates**.

   The **Action Templates Search** page is displayed.

   Alternative methods to open search pages are listed in Section 3.9, "Search, Create, and Import."

## 18.4 Searching for Action Templates

In the Action Templates Search page, you can narrow down the number of action templates that are shown by specifying criteria in the Search Filter.

To search for action templates:

1. Navigate to the **Action Templates Search** page, as described in Section 18.3, "Navigating to the Action Templates Search Page."

   The **Search Results** table will display no results when the **Action Templates Search** page first appears.

2. Specify criteria in the Search Filter to locate the action template.

3. Click **Search**.

   If you do not want to perform the search, click **Reset** to reset the search parameters to the default setting.

The action templates displayed are those that match the criteria specified in the Name, Java Class Name, and Keyword fields (Table 18–1).

*Table 18–1    Action Template Search Filter Criteria*

| Filters and Fields | Descriptions |
| --- | --- |
| Name | Name of the action template. You can enter the complete name or part of an action template name. For example, if you enter new, any action template with new in any part of its name is shown. |
| Java Class Name | The fully qualified classpath of the java class file. |
| Keyword | Keyword in the description. |

Each action template has a name. If the description is too long to be fully shown, you can place the mouse over the text to see the entire description.

By default, action templates are sorted on **Action Template Name**, but you can sort action templates on Description and Java Class name.

In the **Search Results** table, click the row for the action template you are interested in to view more details.

## 18.5 Viewing Action Template Details

In the Results table of the Action Template Search page, click the row of the action template you are interested in to review the details of a specific action template. The

Action Template Details page provides such general details about the case as the Java class name, action name, description, and Java class parameters.

To view details about an action template:

1.  Search for the action template, as described in Section 18.4, "Searching for Action Templates."

2.  In the **Results** table, click the row of the action template you are interested in. The **Action Template Details** page appears.

    The fields are pre-populated with default values.

    You can edit the values of the parameters, action names, and description, but you cannot edit the Java Class name.

## 18.6  Creating a New Action Template

To define a new action template:

1.  Create the Java Class file for the configurable action template.

2.  Copy the Java Class file.

    Now you are ready to create the action template.

    You can create only one action template per class file.

3.  Navigate to the **Action Templates Search** page, as described in Section 18.3, "Navigating to the Action Templates Search Page."

4.  From the **Action Templates Search** page, click **New Action Template**.

    Alternative methods to open create pages are listed in Section 3.9, "Search, Create, and Import."

    The **New Action Template** page appears where you can enter details to create a new action template.

5.  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, see the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

    An example of a Java Class is com.bharosa.vcrypt.tracker.dynamicactions.impl.AddItemToWatchListAction.

    You must enter the *fully qualified* Java class name.

    If you enter an incorrect Java class name, an error occurs when you click **Load Parameters**.

    Also, you must ensure that the Java Class is in the correct directory.

6.  Click **Load Parameters**.

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

    Examples of parameters are shown in the following table.

| Name | Label | Type | Value |
|------|-------|------|-------|
| Item Type | Item Type: | String | <value> |

| Name | Label | Type | Value |
|------|-------|------|-------|
| Watch-List Name | Enter the Watch-List Name: | String | <value> |
| White-List Name | Enter the White-List Name: | String | <value> |
| Black-List Name | Enter the Black-List Name: | String | <value> |

Only one action template can be created per Java Class file. If you try to create an action template using the same Java Class file, a warning appears after you click **Load Parameters**.

7. In the **Action Name** field, enter a name for the action.

8. In the **Description** field, enter a description of the action.

9. Enter values for the parameters.

   All parameter values are required. You cannot save the template until all values are entered.

10. Click **Apply**.

    The message, "Action template created successfully," is displayed.

11. Click **OK** to dismiss the dialog.

After you defined the action templates, the next step is to configure the action instance. A single action template can have multiple instances. For details on configuring the action instance, see Section 18.9, "Creating an Action Instance and Adding it to a Checkpoint."

## 18.7 Navigating to the Action Instances Search Page

You manage configurable actions in Oracle Adaptive Access Manager from the Action Instances Search page. From this page, you can search, view, create, activate, deactivate, and delete action instances.

1. In the Navigation tree, expand **Configurable Actions**.

2. Click **Action Instances**.

   The **Action Instances Search** page is displayed.

   Alternative methods to open search pages are listed in Section 3.9, "Search, Create, and Import."

## 18.8 Searching for Action Instances

In the **Action Instances Search** page, you can narrow down the number of configurable action instances that are shown by specifying criteria in the Search Filter.

To search for action instances:

1. Navigate to the **Action Instances Search** page, as described in Section 18.7, "Navigating to the Action Instances Search Page."

2. Specify criteria in the Search Filter to locate the action instance.

3. Click **Search**.

The action instances shown are those that match the criteria specified in the **Name**, **Checkpoint**, **Keyword**, and **Execution Type** fields (Table 18–2).

*Table 18–2    Action Instances Search Filter Criteria*

| Filters and Fields | Descriptions |
|---|---|
| Name | Name of the configurable action instance. You can enter the complete name or part of a name. |
| Checkpoint | The specified point in a session when rules in a policy are run. For example, at pre-authentication, post-authentication, and in-session. |
| Execution Type | There are two execution types: Synchronous and Asynchronous<br><br>■ Synchronous actions are executed in the order of their priority in the ascending order. For example, if you want to create a CSR case and then send an email with the Case ID, you would choose synchronous actions. Synchronous actions will trigger/execute immediately.<br><br>If the actions are executing in sequential order and one of the actions in the sequence does not trigger, the other actions will still trigger.<br><br>■ Asynchronous actions are queued for execution but not in any particular sequence. For example, if you want to send an email or perform some action and do not care about executing it immediately and are not interested in any order of execution, you would choose asynchronous actions. |
| Keyword | Keyword in the description. |

Each action instance has a name. If the description is too long to be fully shown, you can place the mouse over the text to see the entire description.

In the **Results** table, click the row for the action instance you are interested in to view the **Action Instance Details** page.

## 18.9  Creating an Action Instance and Adding it to a Checkpoint

To create an action instance, follow the procedure in this section.

**Create Action Instance and Associate it to a Checkpoint**

1. Navigate to the **Action Instance Search** page, as described in Section 18.7, "Navigating to the Action Instances Search Page."

2. Click **New Action Instance**.

   Alternative methods to open create pages are listed in Section 3.9, "Search, Create, and Import."

   The **New Action Instance** page is displayed.

3. Next to **Action Instance Template Details**, click **Choose Action Template**.

4. In the **Existing Action Templates** page, select a template and click **OK**.

5. In the **Action Instance** section, enter values for the action instance.

   ■ Name

   ■ Description

   ■ Log Level

     The log level indicates whether the execution status of instance should be recorded.

     – **Disable** turns off logging

     – **Enable** turns on logging

– **Log if error** turns on logging when errors occur

Only if there is an error will the execution status be recorded in the logs. Otherwise, the instance triggering is not recorded in the logs.

■ Checkpoint to associate the configurable actions to

For example, a checkpoint could be Pre-Transaction (a custom checkpoint)

### Choose Execution Type for the Configurable Action

1. Select from two **Execution Types**: "Synchronous" or "Asynchronous."

**Synchronous** actions are executed in the order of their priority in the ascending order.

**Synchronous** is selected as the execution type so that the action is executed immediately after the rules action is triggered.

For the synchronous execution type, if actions are executing in sequential order and one of the actions in the sequence does not trigger, the other actions will still trigger.

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

**Asynchronous** actions are queued for execution and are executed not in any particular sequence.

2. Enter the execution order if execution type is **Synchronous**.

Priority is unique within a checkpoint. An error is displayed when the execution order is not unique.

3. Select **Action Priority** and **Time to Live** if execution type is **Asynchronous**.

Actions are aligned in different queues based on the action priority. When it is time to execute the next action from the queue, the highest-priority action is executed first.

**Time to Live** denotes the maximum time to wait before the action can be discarded.

### Enter Preconditions for the Configurable Action

1. Select the trigger criteria.

Trigger criteria determines when to trigger the action in the session.

The criteria should be either a score or an action or both. These are compared against the values for the selected checkpoint.

■ If the evaluated action matches the action provided, the configurable action is triggered.

■ If the Rules Engine returns a score in the range provided, the configurable action is executed.

For example, if you want to create a case whenever the action type is block, Oracle Adaptive Access Manager will create a case whenever there is an action, "block," in the policy. If you want to create a case whenever the score is greater than 500, Oracle Adaptive Access Manager will create a case when the score is greater than 500 in that particular session.

When both action and score are specified, the configurable action is executed only if both of criteria match with the outcome from the Rules Engine.

2. Enter the values for the action.

   Choose an action. For example, the trigger criteria may be that if the Rules Engine returns "Allow" as the action, the action instance is executed.

   Typical actions from the Rules Engine are "Allow," "Block," "PasswordTextPad," and others.

   In the example, Challenge is selected as the action trigger. When a KBA challenge is returned as a rules result, the configurable action is triggered.

3. Select **Only if this is the final action** if you want the action to be the final action.

   In the example, "Only if this is the final action" is not selected so that the configurable action is triggered for the challenge even though it may not be a final action.

4. Select the score range

   A typical score from the Rules Engine is a numeric value between 0 and 1000.

   Select a range. For example, if the Rules Engine returns a score between "x" and "y," the configurable action is executed.

5. Enter values for all the parameters related to the action.

   For the example, the Watch-List Name is changed to AmtTransferSuspectedList.

**Apply Changes**

To apply the changes:

1. Click **Apply**.

   If the action instance is created successfully, a confirmation appears.

2. Click **OK** to dismiss the dialog.

## 18.10  Creating a Custom Action Instance

To add a custom action instance, you will need to:

1. Develop the action instance by implementing the com.bharosa.vcrypt.tracker.dynamicactions.intf.DynamicAction java interface.

   > **Note:** Implementing means writing java code based on the contract specified by the Java interface com.bharosa.vcrypt.tracker.dynamicactions.intf.DynamicAction.

2. Test the implementation of the action instance thoroughly.

3. Compile the Java class and create a jar file of the compiled class files.

4. Extend/customize Oracle Adaptive Access Manager to add the custom jar.

   Refer to the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager* for steps on adding the custom jar to Oracle Adaptive Access Manager.

5. Restart OAAM Server and OAAM Admin Server.

6. Log in to OAAM Admin and create an action definition entry for the newly deployed configurable action.

7. Make sure all the parameters required for the configurable action are displayed in the user interface.

8. Use the newly available configurable action by adding it to the required checkpoints.

## 18.11 Editing an Action Template

To edit details about a specific action template:

1. Search for the action template, as described in Section 18.4, "Searching for Action Templates."

2. In the **Results** table, click the row of the action template you are interested in. The **Action Template Details** page appears.

   The default values are pre-populated in the **Action Template Details** page.

3. Edit the values of the parameters, action name, and description in the action template.

## 18.12 Exporting Action Templates

To export action templates:

1. Search for the action template, as described in Section 18.4, "Searching for Action Templates."

2. Select the row for each action template you want to export.

3. Click the **Export** button or select **Export Selected** from the **Actions** menu.

4. In the **Export Action Template** dialog, click **Export**.

5. In the **Save** dialog, click **OK**.

## 18.13 Importing Action Templates

To import action templates:

1. Navigate to the **Action Templates Search** page, as described in Section 18.3, "Navigating to the Action Templates Search Page."

2. In the **Action Templates Search** page, click **Import**.

3. In the **Action Templates Import** dialog, click **Browse** and locate the action templates file you want to import.

4. Click **OK**.

## 18.14 Moving an Action Template from a Test Environment

To move an action template from a test environment to a production environment, perform the tasks listed:

1. Export the action template from the test environment. Refer to Section 18.12, "Exporting Action Templates."

2. Import the action template into the target system. Refer to Section 18.13, "Importing Action Templates."

3. If the configurable action is a customized one, skip Steps 1 and 2. Use the OAAM Extensions Shared Library (oracle.oaam.extensions.war) to package the configurable action and related jars and deployed the war into the target system.

   For information on adding custom jars, see "Add Customizations/Extensions using Oracle Adaptive Access Manager Extensions Shared Library" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

   > **Note:** From 11*g*, do not copy the custom jars to OAAM webapp folders.

**Migrating 10*g* Action Templates to 11*g***

In the 11*g* user interface for Action Templates, the Notes field has been removed. If the Notes field contains text in the 10*g* Action Templates, after migration to 11*g*, these notes will be appended (combined) with the description text.

## 18.15 Deleting Action Templates

To delete action templates:

1. Search for the action template, as described in Section 18.4, "Searching for Action Templates."

2. Select the row for each action template you want to delete and click **Delete Action Templates** from the **Actions** menu.

If you select an action template to delete that is used in a checkpoint, an error about the configurable action currently being used by checkpoints is displayed.

When multiple action templates are selected for deletion and if there are checkpoints that contain the instances of some of the action templates selected, a warning message is provided, stating that the instances are linked to Checkpoints and cannot be deleted. You have the option to delete the unlinked action templates.

## 18.16 Viewing a List of Configurable Action Instances

1. Navigate to the Action Instances Search page, as described in Section 18.7, "Navigating to the Action Instances Search Page."

2. In the Search Filter, select a checkpoint to see all the action instances for that checkpoint or select **All** to see all action instances for the checkpoints.

3. Click **Search**.

   In the **Results** table, a list of action instances is displayed.

   If you want to view a particular instance, click the row of the action instance you are interested in. The **Action Instance Details** page appears.

## 18.17 Viewing the Details of an Action Instance

To view the details of an action instance:

1. Navigate to the **Action Instance Search** page, as described in Section 18.7, "Navigating to the Action Instances Search Page."

2. Click the row of the action instance you are interested in viewing.

   The details page of the action instance is displayed.

## 18.18 Editing an Action Instance

To edit an action instance:

1. Navigate to the **Action Instance Search** page, as described in Section 18.7, "Navigating to the Action Instances Search Page."

2. Click the action instance you are interested in editing.

3. In the **Action Instance** section, change the values for the action instance.

   - Name
   - Description
   - Log Level
   - Checkpoint

4. Change the execution type.

5. Change the trigger criteria.

6. Enter values for all the parameters related to the action.

7. Apply the changes.

## 18.19 Deleting an Existing Action Instance

To delete an action instance:

1. Navigate to the **Action Instances Search** page, as described in Section 18.7, "Navigating to the Action Instances Search Page."

2. In the Search Filter, select a checkpoint to see all the action instances for that checkpoint or select All to see all action instances for the checkpoints.

3. Click **Search**.

4. Select the checkbox next to an existing action definition you want to delete.

5. Click **Delete**.

If an action is associated with a checkpoint, you cannot delete it.

## 18.20 Out-of-the-Box Configurable Actions

The following configurable actions are available out of the box:

- CaseCreationAction - Used to create a case

- AddItemToWatchListAction - Used to add item to a watch list.

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

> **Note:** To use system provided configurable actions, you must import the configurable action definition. Refer to Section 2.6, "Importing the OAAM Snapshot."

## 18.20.1 Defining CaseCreationAction

To define CaseCreationAction:

1. Create a case.

   Customer care cases need an owner.

   For information on case creation, see Section 4.8, "Creating a CSR Case."

2. Navigate to the **Action Templates Search** page, as described in Section 18.3, "Navigating to the Action Templates Search Page."

3. From the **Action Templates Search** page, click **New Action Template**.

   The **New Action Template** page appears where you can enter details to create a new action template.

4. Enter the java class name as

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

5. In the **Action Name** field, enter a name for **CaseCreationAction**.

6. In the **Description** field, enter a description for **CaseCreationAction**.

7. For the **Case Type** parameter, enter **1** for "CSR Case."

8. For the **Severity** parameter, enter **1** for "Low", 2 for "Medium", 3 for "High."

9. Enter a value for the **Case Description** that should be set while creating the case.

10. Enter the userId for **Case Creator UserId**. Make sure that userId has a proper role and access permissions for creating the case.

## 18.20.2 Defining AddItemtoListAction

To define AddItemToListAction:

1. Navigate to the **Action Templates Search** page, as described in Section 18.3, "Navigating to the Action Templates Search Page."

2. From the **Action Templates Search** page, click **New Action Template**.

   The **New Action Template** page appears where you can enter details to create a new action template.

3. Enter the Java class name as com.bharosa.vcrypt.tracker.dynamicactions.impl.AddItemToWatchListAction

4. In the **Action Name** field, enter a name for **AddItemToWatchList**.

5. In the **Description** field, enter a description for the action.

6. 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

7. For the **Watch-List Name** parameter, enter the name of the Watch List. Make sure there is a group with the same name.

8. For the **White-List Name** parameter, enter the name of the White List. Make sure there is a group with the same name. Action checks this list before adding an item to Watch List.

   If the item is present in the white list, it will not be added to the watch list.

9. For the **Black-List Name** parameter, enter the name of the Watch List. Make sure there is a group with the same name. Action checks this list before adding an item to Watch List

   If the item is present in the blacklist, it will not be added to the watch list.

## 18.21 Use Cases

This section describes example use cases for configurable actions

### 18.21.1 Use Case: Add Device to Black List

Jeff is a Security Administrator at Dollar Bank. He must configure an action to add a device to a black list group whenever there is a device that has more than three failed login attempts from a blacklisted country within a month.

For example, if there were two login attempts from a device in blacklisted country today and two login attempts two weeks ago from the same device, it would be automatically added to the group by the configurable action.

To configure the action:

1. Search for a device rule that evaluates in-group membership.

   Look for a rule with a maximum count or authentication status check.

2. If a rule does not exist, create one.

   a. Find an existing post-authentication policy used for general security rules.

   b. Create and add the rule.

3. Configure a new trigger action enumeration named add **device to black list** and an action group for it.

4. In the group, add a block action.

5. Configure a configurable action to trigger on **add device to black list** which will add the device to a black list group.

### 18.21.2 Use Case: Add Device to Watch-list Action

Jeff is a Security Administrator at Dollar Bank. He needs to configure an action to add a device to a watch list group whenever there is a device that has more than three failed login attempts within a month. He starts with the rule he will need. He searches for a device rule that evaluates in-group membership. He finds one for device in-group but it does not have a max count or authentication status check. Jeff decides he must create one. He finds an existing post-authentication policy used for general security rules, and then creates and adds the rule. Jeff also configures a new trigger action enumeration named "add device to watch list" and an action group for it. In the group he also adds a block action. Next Jeff configures a configurable action to trigger on "add device to watch list" action which will add the device to a watch list group.

Today there were two login attempts from a device in North Korea and two weeks ago the same device so it was automatically added to the group by the configurable action.

Implementation Notes:

The above requirement can be implemented by following these steps:

1. Create a group called **Device Watch List** that will store the devices that have to be monitored before they can be classified as white-listed or black-listed.

2. Similarly create groups called **Device While List** , **Device Black List**.

3. Create a custom rule action called **add_device_to_watch_list**.

4. Add a rule with the rule condition "USER: Check login count" to a policy for the "PreAuthentication" checkpoint. Configure it such a way that it will trigger and return the action **add_device_to_watch_list** whenever there are more than three failed login attempts within last 30 days.

5. Now create an action instance of the action template **AddItemToWatchListAction** and associate it to the Pre-Authentication checkpoint.

6. Set the trigger criteria as the action by selecting **add_device_to_watch_list** action and set the score range as 0 to 1000.

7. Set the **Item Type** parameter value as **devices** since deviceid needs to be added to the list.

8. Set the **Watch List Name** parameter value as **Device Watch List**.

9. Set the **Black List Name** parameter value as **Device White List**.

10. Set the **White List Name** parameter value as **Device Black List**.

11. Save the action instance

Simulate logins so that the rule triggers and returns **add_device_to_watch_list** as the rule action. Whenever that happens you will see the current device added to the **Device Watch List**.

## 18.21.3  Use Case: Custom Configuration Action

Jeff is a Security Administrator. He has defined a custom configurable action in the test environment. Now he has to export the custom action template from test and import it into Production. (Tip: He has to manually link the custom jar (custom class) before the import action, if not import would fail. In 11*g*, he does this by adding his custom jars to the OAAM Extensions Shared Library. The server should be restarted for the changes to take effect)

Implementation Notes:

The above can be achieved by following these steps:

1. Jeff implements his custom configurable action by writing a java class that implements `com.bharosa.vcrypt.tracker.dynamicactions.intf.DynamicAction` java interface.

2. He can compile his class by linking the Oracle Adaptive Access Manager jars from `$IDM_ORACLE_HOME\oaam\native\java\lib` folder.

3. He should then test his custom configurable action to make sure it is working correctly.

4. He should then package his class as a jar file and create the shared library by following the structure of the OAAM Extensions Shared Library that is available in `$IDM_ORACLE_HOME\oaam\oaam_extensions\generic` folder

5. He should then overwrite the existing oracle.oaam.extensions shared library or deploy his extensions shared library with a different implementation version.

6. He can then create action template and an action instance for the custom configurable action.

7. He should test it by creating an action instance and attach it to a checkpoint and set the trigger criteria and then simulate logins/sessions from OAAM Server to trigger the custom configurable action.

8. Once he is done with testing, he can export his custom action template.

9. Now he has export file that has the custom action template and also the shared library that has custom java code related to his custom configurable action.

10. He can deploy his custom configurable action by redeploying the OAAM Extensions Shared Library using his shared library and then import his custom configurable action template from his export file.

## 18.21.4 Use Case: Create Case

Matt is a Security Administrator. He needs a configurable action such that an Agent case is created automatically, whenever a user is blocked more than 3 times in the last one month. The Fraud investigator will work on these cases to determine if the user is a risky user.

Implementation Notes:

The above requirement can be implemented by following these steps:

1. Create a custom rule action called **create_agent_case**.

2. Add a rule with the rule condition "USER: Check login count" to a policy for the Post-Authentication checkpoint. Configure it such a way that it will trigger and return the action **create_agent_case** whenever there are more than three blocks for the user within last 30 days.

3. Now create an action instance of the action template **CaseCreationAction** and associate it to the Post-Authentication checkpoint.

4. Set the trigger criteria as the action by selecting **create_agent_case** action and set the score range as 0 to 1000.

5. Set the parameters of **CaseCreationAction** as follows:

    a. Enter "2" as value of **Case Type** parameter

    b. Enter "2" (for Medium) or "3" (for High) as **Severity** parameter value

    c. Enter "Case Description" parameter value.

    d. Enter the userId for "Case Creator UserId" parameter. Make sure that userId has a proper role and access permissions for creating the case

6. Save the action instance.

7. Try few logins for a user so that it triggers and returns at least three blocks

8. After third block, you should see automatic creation of an agent case by the configurable action.

# 19

# Predictive Analysis

Oracle Adaptive Access Manager's Predictive Analysis feature compliments configurable rules and behavioral profiling by enabling you to perform statistical risk analysis in real time using its out-of-the-box predictive analytic application that integrates ODM features, such as data mining and data analysis algorithms. Risk analysis is trained over time.

This chapter contains the following sections:

- Important Terms
- Prerequisites
- Initial Setup
- Rebuild the ODM Models to Provide Feedback and Update Training Data
- Policy Evaluation
- Tuning the Predictive Analysis Rule Conditions
- Adding Custom Database Views
- Adding Custom Grants
- Adding New ODM Models
- Adding Custom Input Data Mappings

## 19.1 Important Terms

Important terms for predictive analysis are presented in this section.

### 19.1.1 Predictive Analysis

Predictive analytics encompasses a variety of techniques from statistics, data mining and game theory that analyze current and historical facts to make predictions about future events.

- Individual User Behavior Profiling: End user login behaviors are evaluated to determine how abnormal it is currently compared to their own past behavior, if there is past behavior captured.

- Individual Device Profiling: Devices used for login have behavior that is evaluated to determine how abnormal it is currently compared to their own past behavior if past behavior has been recorded.

- New Device Profiling: If a device does not have any historical data to profile then predictive techniques are used to determine how risky the device is.

- User Type and Location Profiling: Predictive models evaluate the degree of anomaly based on the type of user (groups, Organization ID) rather than each individual user.

- User Type and Time Profiling: Similar to location profiling, time profiling uses predictive techniques to identify anomalies in behavior when there is not much historical data for the specific user but there is production data related to users of the same type.

### 19.1.2 Data Mining

Data mining is the practice of automatically searching large stores of data to discover patterns and trends that go beyond simple analysis. Data mining uses sophisticated mathematical algorithms to segment the data and evaluate the probability of future events. Data mining is also known as Knowledge Discovery in Data (KDD).

Data mining can answer questions that cannot be addressed through simple query and reporting techniques.

### 19.1.3 ODM

Oracle Data Mining (ODM) is an option that extends Oracle Database 11g Enterprise Edition's out-of-the-box capabilities. ODM implements data mining and data analysis algorithms for prediction and anomaly detection and enables deployment of data mining models inside the database. The ODM option is not a separate component; functionality is built into the Oracle database kernel and operates on data stored in the database tables. There is no need to move data out of the database into files for analysis and then back from files into the database for storing. The data never leaves the database -- the data, data preparation, model building, and model scoring results all remain in the database.

### 19.1.4 Predictive Models

Predictive models are supervised learning functions. Using predictive models, OAAM fine tunes its analysis; the more each model is trained, the more accurate the risk analysis becomes. The out-of-the-box predictive models are trained in two ways: the anomaly detection model trains automatically when fed historical access data, and the fraud classification model trains on the findings of human fraud investigators. You can configure additional models as required to meet specific deployment use cases. This approach to predictive risk analysis allows you to clearly see on which decisions outcomes are based and allows augmentation as required.

## 19.2 Prerequisites

Make sure the following prerequisites are met before you activate the Predictive Analysis functionality:

- Oracle 11g Enterprise Edition version of the database is being used

- Oracle Data Mining (ODM) option

- Identity Management Suite is installed

- A reasonable amount (at least 100) of OAAM sessions exists that represent a variety of usual OAAM sessions

- At least 100 or more sessions exist that are classified as "Fraud" and "Not Fraud" using the Agent Case functionality.

> **Note:** To mark a session as Fraud/Not Fraud, create an agent case link the session and close the Agent case with Disposition as either "Confirmed Fraud" or "Not Fraud".

For testing purposes remember the criteria for marking sessions as "Fraud" or "Not Fraud" since the ODM (Oracle Data Mining) model will use that as the training data.

## 19.3  Initial Setup

1.  Create an ODM database user. Execute the SQL script `create_odm_user.sql`.

    When it prompts for inputs, enter the ODM user name as the value of first parameter and then the password of ODM User as the value of second parameter.

    The script is located in the `$MW_HOME\oaam\cli\odm` folder.

2.  Set up the OAAM CLI environment. Make sure you have added the following to the CSF/Credential Store using Enterprise Manager:

    a.  OAAM DB User Name and Password with **oaam_db_key** as the keyname under the map **oaam**.

    b.  ODM DB User Name and Password with **oaam_odm_db_key** as the keyname under the map **oaam**.

    c.  Set the property `oaam.db.url` with the JDBC URL of the OAAM database in `oaam_cli.properties`.

3.  By default Predictive Risk uses the OAAM_CLASSIFIED_REQUEST_VIEW. For predictive risk to work for sessions from non-flash devices you need to use "OAAM_CLASSIFIED_REQ_NOFLASH_VW".

    OAAM_CLASSFIED_REQ_NOFLASH_VW view has all the requests (both flash and no-flash).

    To set the OOTB ODM Model "OAAM Fraud Request Model" to use the no-flash data set the following properties before running initODM.sh:

    ```
    oracle.oaam.odm.model.enum.oaam_fraud_request_model.data_table_name=OAAM_
    CLASSFIED_REQ_NOFLASH_VW
    oracle.oaam.odm.model.enum.oaam_fraud_request_model.inputdata_
    mapping=oracle.oaam.odm.datamapping.enum.user_request_data_noflash
    ```

4.  Run the shell script **initODM.sh** in the OAAM CLI folder. This script does the following:

    ■ Seeds the ODM tables that have the normalized data of the browser and flash fingerprints

    – OAAM_DEVICE_BROWSER_FPRINTS

    – OAAM_DEVICE_FLASH_FPRINTS

    ■ Creates the following database views that are used as input data by the ODM models:

    – OAAM_CLASSIFIED_REQUESTS_VW

    – OAAM_INVESTIGATED_REQUESTS

    – OAAM_UNCLASSIFIED_REQUESTS_VW

–   OAAM_CLASSIFIED_REQ_NOFLASH_VW

–   OAAM_UNCLASSIFIED_REQ_NOFLASH_VW

■   Creates the following ODM Models if required data is present:

–   OAAM_ANOMALY_REQUEST

–   OAAM_FRAUD_REQUEST

5.   Log in to **OAAM Admin Server** and link the Predictive Analysis Policy to **All Users** or the required user groups.

6.   Log into WebLogic Admin Server using the WebLogic Console and create a **DataSource** with JNDI name such as **jdbc/OAAM_SERVER_ODM_DS** and point it to the ODM DB User and add the Managed server of **OAAM Server** as the **target**.

7.   Restart OAAM Server since ODM initialization updates some enum-related properties.

8.   To test anomaly detection, try to log in from a different kind of browser or location which is not yet present in the OAAM database.

9.   To test "fraudulent session prediction" functionality, log in in a similar session that is linked to an Agent case which is closed with the **Confirmed Fraud** disposition.

**OAAM_CLASSFIED_REQ_NOFLASH_VW**

By Default Predictive Risk uses the OAAM_CLASSIFIED_REQUEST_VIEW. For predictive risk to work for sessions from non-flash devices you need to use "OAAM_CLASSIFIED_REQ_NOFLASH_VW".

OAAM_CLASSFIED_REQ_NOFLASH_VW view has all the requests (both flash and no-flash).

To set the OOTB ODM Model "OAAM Fraud Request Model" to use the no-flash data set the following properties and run initODM.sh:

```
oracle.oaam.odm.model.enum.oaam_fraud_request_model.data_table_name=OAAM_
CLASSFIED_REQ_NOFLASH_VW
oracle.oaam.odm.model.enum.oaam_fraud_request_model.inputdata_
mapping=oracle.oaam.odm.datamapping.enum.user_request_data_noflash
```

## 19.4 Rebuild the ODM Models to Provide Feedback and Update Training Data

Important points about rebuilding the ODM models are presented in this section.

■   Rebuilding the ODM models is one way to provide feedback to ODM with latest case creation data so that sessions can be appropriately flagged.

■   You can rebuild the ODM models at regular intervals so that ODM models are trained with the latest data in OAAM.

■   Based on the volume of requests, you can determine the frequency of rebuilding the models. It is recommended to rebuild the models every month at the end of the month.

■   You can set the date range of requests that have to be considered by the ODM models by setting the property `oracle.oaam.predictive_analysis.request.period` as follows:

- – Format of value is `<Number of Years>,<Number of Months>,<Number of Days>,<Number of Hours>`

  – **Examples:**

    * Everything can be indicated using 0 (zero). Use this option with caution, if there are more than a couple of million OAAM requests this could result in a very high model build times and DB errors related to out-of-memory.

    * Last two years can be indicated using **2,0,0,0** or just **2**.

    * Last two years and three months can be indicated using **2,3,0,0** or just **2,3**.

    * Last 3 days can be indicated using **0,0,3,0**

    * Last four hours can be indicated using **0,0,0,4**

- Setup OAAM CLI environment and run the script `initODM.sh`.

## 19.5 Policy Evaluation

The following steps describe the flow of Predictive Analysis evaluation:

1. OAAM User Request goes for Post-Authentication checkpoint evaluation.

2. Predictive Analysis policy executes as part of Post-Authentication.

3. The **Check if the current request is fraudulent rule** is executed. As part of the execution it takes the required classification type and values of attributes from current request and executes the ODM SQL function prediction_probability() with the given model name. This call returns a prediction probability value which is tested to see if it falls in the given range. If so then the OAAM Suspicious Fraudulent Request alert is generated and risk score is set to **1000**.

4. The **Check if the current request is anomalous** rule is executed. As part of the execution it takes values of attributes from current request and executes the ODM SQL function prediction_probability() with the given model name. This call returns a prediction probability value which is tested to see if it falls in the given range. If so then the OAAM Anomalous Request alert is generated and the risk score is set to **1000**.

## 19.6 Tuning the Predictive Analysis Rule Conditions

The following parameters of Predictive Analysis rule conditions can be tuned/changed:

- ODM Model Name that is used for evaluation/scoring

- Range of prediction probability to trigger the rule condition

- Default return value in case of errors

- Classification Type (applies only to the **Check Fraudulent User** rule condition)

To set the above parameters you can go to the **Predictive Analysis Policy** and navigate to the required rule and update the parameters.

> **Note:** The following sections describe advanced functionality which is typically performed by integrators who have Java coding knowledge and knowledge of both OAAM and ODM.

## 19.7 Adding Custom Database Views

- Add the custom view definitions to `$MW_HOME\oaam\cli\odm\custom_oaam_odm_views.sql`.

---

**Note:** Make sure the view definition SQL ends with ";" and there are no extra lines or comments in the file

---

- If you do not want to hard-code the OAAM DB User name then use the variable <oaam_user> wherever you refer to the OAAM schema. This will be replaced with the actual OAAM DB user name by `initODM.sh` when you run it next time.

- When you run `initODM.sh` the next time, it will execute the SQL statements in `custom_oaam_odm_views.sql` that will create the custom views.

## 19.8 Adding Custom Grants

- Add the SQL statements that grant select access OAAM tables to the file `$MW_HOME\oaam\cli\odm\custom_oaam_grants_to_odm_user.sql`.

---

**Note:** **Note:** Make sure the view definition SQL ends with ";" and there are no extra lines or comments in the file

---

- If you do not want to hard-code the ODM DB User name then use the variable <odm_user> wherever you refer to ODM DB User. This will be replaced with actual ODM DB user name by `initODM.sh` when you run it next time.

- When you run `initODM.sh` next time, it will execute the SQL statements in `custom_oaam_odm_views.sql`.

## 19.9 Adding New ODM Models

To add a new ODM Model, follow these steps:

1. Determine the type of model. Currently OAAM supports only CLASSIFICATION models.

2. Determine if the existing ODM view can be used to build the model. If not, create a new view and add that definition to `$MW_HOME\oaam\cli\odm\custom_oaam_odm_views.sql`.

   ---

   **Note:** Make sure the view definition SQL ends with ";" and there are no extra lines or comments in the file.

   ---

3. Determine if any of your new views require additional grants to access the OAAM tables or any custom tables. Add those custom grants to `$MW_HOME\oaam\cli\odm\custom_oaam_grants_to_odm_user.sql`.

   ---

   **Note:** Make sure the grant statements end with ";" and there are no extra lines or comments in the file.

   ---

4. Create a new ODM model using Oracle Data Miner or using the SQL command call dbms_data_mining.drop_model(). Refer to ODM documentation for details.

5. Test your ODM model using sample data. You can typically do this by executing the following:

   ■ For anomaly detection models:

   Select prediction_probability(<model_name>, '0' using <value1> as attribute1, <value2> as attribute2, …. <valueN> as attributeN> from dual

   ■ For other classification models:

   Select prediction_probability(<model_name>, <classificationValue> using <value1> as attribute1, <value2> as attribute2, …. <valueN> as attributeN> from dual

6. Once you are done with testing, add a new enum element to oracle.oaam.odm.model.enum with the following properties:

*Table 19–1 Properties for oracle.oaam.odm.model.enum*

| Property Name | Notes |
|---|---|
| name | Name of the model |
| description | Description of the model |
| type | Type of the model.<br>**Anomaly Detection:** oracle.oaam.odm.modeltypes.enum.oneclasssvm<br>**Classification:** oracle.oaam.odm.modeltypes.enum.classification |
| odm_model_name | Exact name of the ODM model. The OAAM setup script uses this to create the ODM model. |
| data_table_name | Exact name of the input data table/view name. The model will be built using this table/view name. |
| case_id_column | Column in the data table/view that uniquely identifies each row. |
| target_column | Do not specify this for Anomaly Detection models. For classification models, specify the column whose value has to be predicted. Typically this column should have the values ('fraud' or 'not_fraud') as mentioned in the oracle.oaam.odm.fraud_classification_types.enum' |
| settings_table_name | Name of the database table that has settings for the ODM model. You can use the existing tables 'OAAM_ANOMALY_MODEL_SETTINGS' for Anomaly Detection models and 'OAAM_ANOMALY_MODEL_SETTINGS' for Classification models if you don't have any explicit settings. |
| inputdata_mapping | Specify how the input required for evaluation/scoring is mapped to OAAM Data. You can use the following existing mappings if you do not have any new requirements. Otherwise refer to Section 19.10, "Adding Custom Input Data Mappings":<br>oracle.oaam.odm.datamapping.enum.user_request_data<br>oracle.oaam.odm.datamapping.enum.user_request_data_noflash |
| is_available | Set it as 'false' so that initODM.sh script can build the ODM model and set this value to 'true'. If you already built the ODM model by yourself then set this value to 'true' so that the OAAM rules can use this model to evaluate/score against input data. |

## 19.10 Adding Custom Input Data Mappings

This section contains information about adding custom input data mappings.

### 19.10.1 When to Use

Custom input data mappings are needed if any of the following conditions apply:

- You want to use fewer attributes (than what is available out-of-the-box) to evaluate/score the out-of-the-box ODM models

- You want to create a custom ODM model based on custom table/view that has different set of attributes than the existing input data mappings.

### 19.10.2 Using OAAM Attributes to Build a Custom Input Data Mapping

You can use existing OAAM attributes and create custom input data mappings. This approach is useful if you are reusing the existing database view that uses OAAM request data that includes session, browser-fingerprint, flash-fingerprint, and location data.

Steps to create an input data mapping are as follows:

1. Add a new enum element to `oracle.oaam.odm.datamapping.enum`.

2. Set the `inputdata_mapping` property of model enum element to point to the newly added enum element.

3. Add the required list of name-values from the following list to the newly added enum element:

    - request_minute=request.minute

    - request_hour=request.hour

    - request_day_of_week=request.day_of_week

    - request_day_of_month=request.day_of_month

    - request_day_of_year=request.day_of_year

    - request_week_of_month=request.week_of_month

    - request_week_of_year=request.week_of_year

    - request_month=request.month

    - request_quarter=request.quarter

    - request_year=request.year

    - auth_status=request.auth_status

    - user_identifier=request.user_identifier

    - login_id=request.login_id

    - user_group_id=request.user_group

    - request_ip_address=request.ip_address

    - is_registered=request.is_registered

    - auth_client_type=request.auth_client_type

    - secure_client_type=request.secure_client_type

    - pre_auth_action=request.pre_auth_action

    - post_auth_action=request.post_auth_action

    - device_id=device.device_id

    - device_cookie_disabled=device.cookie_disabled

- device_flash_disabled=device.flash_disabled

- browser_country=browser.country

- browser_language=browser.language

- browser_language_variant=browser.language_variant

- browser_name=browser.browser_name

- browser_operating_system=browser.os

- browser_user_agent_string=browser.user_agent_string

- audio_video_disabled=flash_fingerprint.audio_video_disabled

- has_accessibility=flash_fingerprint.has_accessibility

- has_audio=flash_fingerprint.has_audio

- has_audio_encoder=flash_fingerprint.has_audio_encoder

- embedded_video=flash_fingerprint.embedded_video

- has_ime_installed=flash_fingerprint.has_ime_installed

- has_mp3=flash_fingerprint.has_mp3

- supports_printer=flash_fingerprint.supports_printer

- supports_screen_broadcast=flash_fingerprint.supports_screen_broadcast

- supports_playback_screen_brd=flash_fingerprint.supports_playback_screen_brd

- supports_streaming_audio=flash_fingerprint.supports_streaming_audio

- supports_streaming_video=flash_fingerprint.supports_streaming_video

- supports_native_ssl=flash_fingerprint.supports_native_ssl

- contains_video_encoder=flash_fingerprint.contains_video_encoder

- debug_version=flash_fingerprint.debug_version

- flash_language=flash_fingerprint.flash_language

- is_local_file_read_disabled =flash_fingerprint.is_local_file_read_disabled

- manufacturer=flash_fingerprint.manufacturer

- flash_operating_system =flash_fingerprint.flash_operating_system

- aspect_ratio_of_screen =flash_fingerprint.aspect_ratio_of_screen

- player_type=flash_fingerprint.player_type

- is_color_screen=flash_fingerprint.is_color_screen

- dots_per_inch=flash_fingerprint.dots_per_inch

- screen_resolution=flash_fingerprint.screen_resolution

- flash_version=flash_fingerprint.flash_version

- country_id=location.country_id

- state_id=location.state_id

- city_id=location.city_id

- metro_id=location.metro_id

- isp_id=location.isp_id

- routing_type=location.routing_type

- connection_type=location.connection_type

- connection_speed=location.connection_speed

- top_level_domain=location.top_level_domain

- sec_level_domain=location.secondary_level_domain

- asn=location.asn

- carrier=location.carrier

- zip_code=location.zip_code

- region_id=location.region_id

- phone_area=location.phone_area

### 19.10.3 Using Custom Attributes to Build a Custom Input Data Mapping

If you want OAAM to use custom attributes while evaluating/scoring an ODM model then you can develop custom java class that can be used to get values of the custom attributes.

Follow these steps to use custom attributes for building and evaluating ODM models

1. Add a new enum element to 'oracle.oaam.predictive_analysis.attribute_resolvers.enum'.

2. Add 'class' property with value as the fully qualified class name of the Java class that will have logic to return values for the custom attributes.

3. Add all the custom attributes as properties to the newly added enum element. Value of these properties can be the name/description of the attribute. Do not use 'name', 'description', 'class' as attribute names.

4. Develop the custom Java class that handles custom attributes.

   - It should extend the OAAM class oracle.oaam.integration.datamining.rules. OAAMAttributesResolver

   - It should implement a public constructor that takes requestId as the parameter. That constructor should call the super constructor.

   - It should extend the method **public Object getValue(String attributeName)** and have logic to return the value of given attribute. AttributeName will be in the format of '<enumElement>.<property>'

   - Deploy the custom Java class as an OAAM Extension using OAAM Extensions Shared Library. Refer to Developer Guide for deploying OAAM Extensions.

5. If you are using a custom database view then add a custom mapping by adding new enum element to 'oracle.oaam.odm.datamapping.enum' enum and add all the column names of the database view as properties to this enum element. Add the related custom attribute name as the value for these properties. Value should be in the format of <enumElement>.<property>.

6. If you are not using custom database view but just want to create custom mapping of existing request data then pick the required columns from the following and add them to your custom mapping enum element:

*Table 19–2    Custom Mapping*

| A | B | C |
| --- | --- | --- |
| request_minute | device_flash_disabled | flash_language |
| request_hour | browser_country | is_local_file_read_disabled |
| request_day_of_week | browser_language | manufacturer |
| request_day_of_month | browser_language_variant | flash_operating_system |
| request_day_of_year | browser_name | aspect_ratio_of_screen |
| request_week_of_month | browser_operating_system | player_type |
| request_week_of_year | browser_user_agent_string | is_color_screen |
| request_month | audio_video_disabled | dots_per_inch |
| request_quarter | has_accessibility | screen_resolution |
| request_year | has_audio | flash_version |
| auth_status | has_audio_encoder | country_id |
| user_identifier | embedded_video | state_id |
| login_id | has_ime_installed | city_id |
| user_group_id | has_mp3 | metro_id |
| request_ip_address | supports_printer | isp_id |
| is_registered | supports_screen_broadcast | routing_type |
| auth_client_type | supports_playback_screen_brd | connection_type |
| secure_client_type | supports_streaming_audio | connection_speed |
| pre_auth_action | supports_streaming_video | top_level_domain |
| post_auth_action | supports_native_ssl | sec_level_domain |
| device_id | contains_video_encoder | asn |
| device_cookie_disabled | debug_version | carrier |
| | | zip_code |
| | | region_id |
| | | phone_area |

# Part VI

## Managing Transactions

This part of the book contains information about managing transactions in Oracle Adaptive Access Manager.

It contains the following chapters:

- Chapter 20, "Creating and Managing Entities"
- Chapter 21, "Managing Transactions"

# 20

# Creating and Managing Entities

A transaction is a process such as bill pay, wire transfer, address change, and so on. The core elements of an Oracle Adaptive Access Manager transaction are entities and transaction data. Entities can be defined and associated as an instance of a transaction.

This chapter provides information on creating, editing, activating and deactivating, and importing and exporting entities.

## 20.1 Introduction and Concepts

This section introduces you to the concept of entities.

### 20.1.1 Entities

An **Entity** is a user-defined data structure, which comprises of a set of attributes. The entity can be re-used across different transactions. An example of an entity is an address. When associating the entity with a transaction you can create a shipping address and billing address from the address entity.

*Figure 20–1 Address Entity*
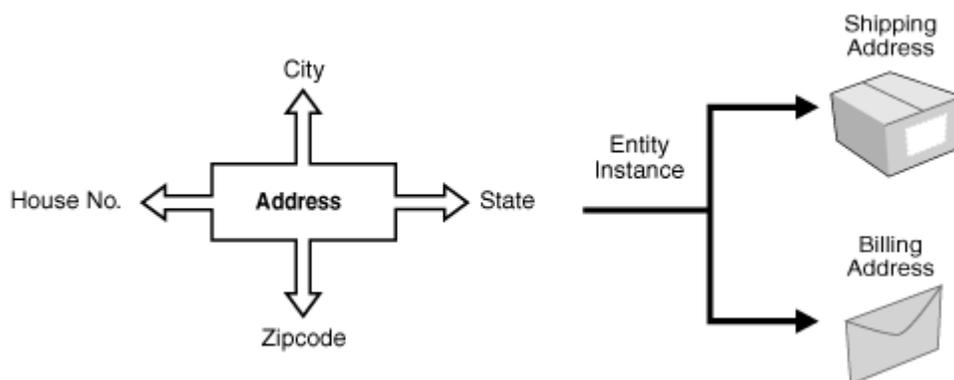


### 20.1.2 Data Elements

Data elements are used to describe the attributes that make up an entity. For example, the credit card entity has attributes such as address line 1, address line 2, city, zip, and state. Data elements, such as description, length, type, and so on, are used to describe each attribute.

### 20.1.3 Display Element

Display elements are the elements you want to present and the order in which you want to present the value of an entity in a user interface. For example, if you want to display an address, you would want to show address line 1 as the first item, address line 2 as the second item, city as the third item, state as the fourth item, and zipcode as the fifth item.

### 20.1.4 ID Scheme

An ID scheme consists of the data elements that can uniquely identify an entity, in other words, you are defining the unique combination that identifies the entity. For example, the credit card entity has many attributes, but the way to uniquely identify a credit card is by using the 16-digit credit card number. In that case, the ID scheme is just the credit card number.

Another example, the address entity has address line 1, address line 2, city, state, and zipcode as attributes. Address line 1, address line 2, and zipcode, without the state and city attributes, can still be used to identify the address uniquely.

### 20.1.5 Internal ID

The internal identifier used to identify a data element in the entity. It is created based on the display name. For example, if Address Line 1 is the display name, spaces between words are replaced by decimals to create an internal ID.

Examples of internal IDs are Address.Line.1, Address.Line.2, or Zip.Code.

The IDs are automatically created for you.

### 20.1.6 External ID

The client supplies the Ext ID value. Oracle Adaptive Access 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 already have IDs with the client.

## 20.2 Navigating to the Entities Search Page

To navigate to the Entities Search page, double-click **Entities** in the Navigation tree.

Alternatively, you can:

- Right-click **Entities** in the Navigation tree and select **List Entities** from the context menu.

- Select **Entities** in the Navigation tree and then choose **List Entities** from the **Actions** menu.

- Click the **List Entities** button in the Navigation tree toolbar.

The Entities Search page is the starting place for managing entities. From the Entities Search page, you can:

- Search for entities

- Create new entities

- Import/export entities

- Activate/deactivate entities

- Delete entities
- Open the Entity Details page

An example of an **Entities Search** page is shown in Figure 20–2.

*Figure 20–2   Entities Search page*



## 20.3  Searching for Entities

To search for entities:

1. Navigate to the **Entities Search** page, as described in Section 20.2, "Navigating to the Entities Search Page."

2. Specify criteria in the Search Filter to locate the entity.

   The search filter criteria are described in Table 20–1.

*Table 20–1      Search Filter Criteria*

| Field | Description |
| --- | --- |
| Name | The name of the entity. |
| Description keyword | The description keyword |
| Status | The status of the entity. |

3. Click **Search**.

The **Search Results** table displays a summary of entities that match the criteria specified in the **Name**, **Description Keyword**, and **Status** fields.

There is a link on the entity name. To view the entity details, click the link.

## 20.4 Creating an Entity

Follow the steps in this section to create a new entity. You will have to provide the required information for all tabs of the Entities Details page before you can activate the entity.

> **Note:** After creating an entity, you must activate it if you want to use it in a transaction. Only active entities can be used in a transaction. By default an entity is disabled when it is created. For information on activating an entity, refer to Section 20.9, "Activating Entities."

### 20.4.1 Initial Steps

To create an entity, follow these steps.

1. Navigate to the **Entities Search** page, as described in Section 20.2, "Navigating to the Entities Search Page."

2. In the **Entities Search** page, click the **New Entity** button.

   Alternative methods to open create pages are listed in Section 3.9, "Search, Create, and Import."

   An example of a **New Entity** page is shown in Figure 20–3.

*Figure 20–3   New Entity Page*



3. In the **New Entity** page, enter a unique entity name.

4. Enter a description about the data element. For example, you can enter "Credit card number of customer" or "Account number of customer."

5. Click **Apply**.

   A confirmation dialog appears with a message that the entity was created successfully.

6. Click **OK** to dismiss the dialog.

   The **Entity Details** page appears for the entity that you have just created.

   The page contains four tabs:

- **Summary** - General Details

- **Data** - Data Elements (Used for adding and editing data elements of entity)

- **ID Scheme** - Data Elements (Used for adding and editing data elements of an entity)

- **Display** - Display Elements (Used for adding and editing display elements of the entity based on the Identification Scheme)

The tab titles for Data, ID Scheme, and Display will show the number of data elements present, in parenthesis, when you have added your elements.

## 20.4.2 Adding and Editing Data Elements

The **Data** tab is used for adding and editing data elements of an entity.

In the **Data** tab, specify the data elements that are part of that entity.

For example, for an entity like Address, the elements are Address Line 1, Address Line 2, City, State and Zip code. Metadata elements, such as a label, description, data type, and so on, describe these elements of the entity.

Define the data elements for each element by following these instructions:

1. Enter a label.

   For example, Address Line 1, Address Line 2, City, or Zip code.

2. Enter a description about the data element.

   Data elements are the attributes of an entity.

   For example, the address of the customer logging in.

3. Specify whether the element is required.

   Some data elements are not populated all the time because the entity can function without this data. Those elements are marked as "not required." For example "Address Line 2" in an address is not required since many addresses do not have "Address Line 2."

4. Specify whether the element should be encrypted.

   If **Is Encrypted?** is set to **True**, data is encrypted so that it can be stored securely in the database; thereby protecting sensitive data.

   Encrypted fields have the following constraints:

   - These fields should not be used in rules. If they are used, you cannot specify regular values for comparing against these fields; the values will have to be encrypted values.

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

     Numeric fields cannot be encrypted.

   Encrypted fields can be displayed in OAAM Admin.

5. Specify the data element Data Type.

   For example, String.

6. If you want to add another element, click the **Add** button on the toolbar and repeat Steps 1 through 7.

7. Click **Save**.

You can use the **Delete** button to delete the data elements within the entity.

> **Note:**  The **Row and Column** values are automatically assigned based on the data type and should not be changed unless you want to rearrange values in the database.

### 20.4.3  Selecting Elements for the ID Scheme

In the **ID Scheme** tab, select the elements that you want to use to uniquely identify an entity.

For example, the credit card entity has many attributes, but the way to uniquely identify a credit card is by using the 16-digit credit card number. In that case, the ID scheme is just the credit card number.

Another example, the address entity has Address Line 1, Address Line 2, City, State, and Zip code as attributes. The Address Line 1, Address Line 2, and Zip code attributes can be used to identify the address uniquely. The State and City attributes are not necessary.

Address Line 1 alone would not uniquely identify an address. For example, 150 Main Street can exist in more than one location.

An example of a **ID Scheme** tab is shown in Figure 20–4.

*Figure 20–4  ID Scheme tab*
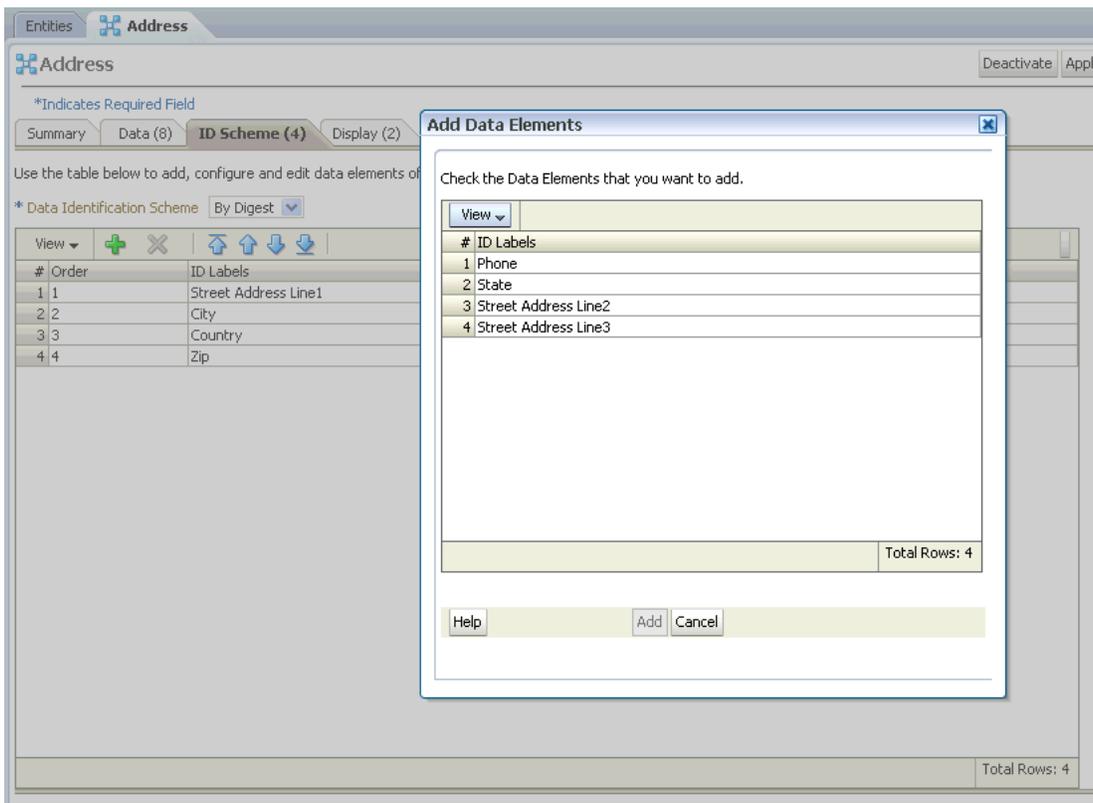


1.  Select the **Data Identification Scheme**.

Identification Scheme determines how an entity is uniquely identified using the elements that are part of the entity. The elements that are selected should be stored as plain text (**key**) or encrypted (**digest**).

- **By Key**: This scheme creates a unique identifier by simply concatenating the selected elements of the entity.

- **By Digest**: This scheme creates a unique identifier by hashing the values of the selected elements of the entity. The resultant key is usually cryptic. Use this scheme when the data values are large or if they need to be secured.

2. Click the **Add** button on the toolbar to add a data element.

3. In the **Add Data Elements** screen, select the data elements to add to the ID Scheme and click **Add**.

   You can select one or several data elements to add to the identification scheme.

   For example, you only need the 16-digit credit card number to identify the credit card.

   After the data elements are added, they are not available in the list for further selection.

4. Select the order of the elements

   The order determines how the data is concatenated while forming the data that identifies the entity. Order is not required and is automatically pre-filled if you do not fill in that information.

You can use the **Delete** button to delete the data elements within the entity.

### 20.4.4 Specifying Data for the Display Scheme

In the **Display** tab, define the **display scheme**. The display scheme specifies the data elements to present and their order when you display the value of the entity in reports:

- The data elements form the entity data that can be displayed.

- The order determines how the data is concatenated while forming the data to be displayed for the entity

An example of a **Display** tab is shown in Figure 20–5.

**Figure 20–5  Display tab**
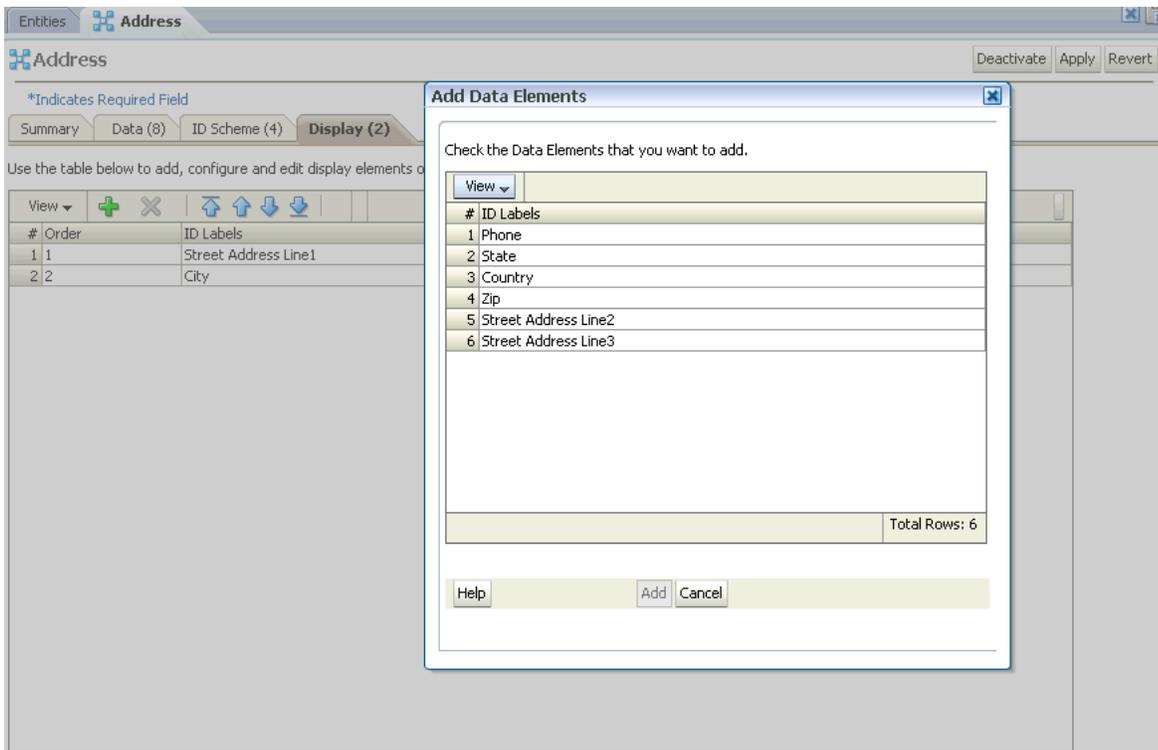


The Data elements that you have selected to present are shown in the **Transaction Details** page.

To select the data elements, follow these steps.

1. Click the **Add** button to add a data element.

2. In the **Add Data Elements** screen, select the data elements to add for displaying and click **Add**.

   For example, for an address, you can choose to present Address Line 1, City, State, and Zip code.

3. Select the order of the elements

   The order determines what is shown first, second, third, and so on when the data is displayed for the entity. Order is not required and is automatically pre-filled if you do not fill in that information.

   For example, if you want to display an address, you would want to show address line 1 as the first item, address line 2 as the second item, city as the third item, state as the fourth item, and Zip code as the fifth item.

You can use the **Delete** button to delete the display elements.

## 20.4.5  Activating the Entity

After creating an entity, you must activate it if you want to use it in a transaction. Only active entities can be used in a transaction. By default an entity is disabled when it is created. For information on activating an entity, refer to Section 20.9, "Activating Entities."

## 20.5 Viewing Details of a Specific Entity

To view the details of a specific entity:

1. Navigate to the **Entities Search** page, as described in Section 20.2, "Navigating to the Entities Search Page."

2. From the **Entities Search** page, search for the entity you want.

   The filters are described in Table 20–1.

3. In the **Results** table, click the entity name.

   An example of an **Entity Details** page is shown in Figure 20–6.

*Figure 20–6  Entity Details page*



## 20.6 Editing the Entity

To edit the details of a specific entity:

> **Note:** Be cautious when editing entities. If you edit an entity and it is in several transactions, then the edits are applied to all instances of the entity in the different transactions.

1. If you are not on the **Entity Details** page of the entity you want to edit, follow the instructions in Section 20.5, "Viewing Details of a Specific Entity."

2. From the **Summary** tab, you can modify the name and description of the entity; and activate or deactivate the entity.

3. From **Data** and **ID Schemes** tabs, you can modify the data elements of the entity.

   If you delete a data element from the scheme, it is added to the **Add** list and available the next time you select **Add Data Elements**.

4. From the **Display** tab, you can edit the way the entity is displayed.

5. Click **Apply**.

## 20.7 Exporting Entities

To export entities:

1. Navigate to the **Entities Search** page, as described in Section 20.2, "Navigating to the Entities Search Page."

2. In the **Entities Search** page, enter the search criteria you want and click **Search**. Refer to Section 20.3, "Searching for Entities."

3. Select the row for each entity you want to export.

4. Click the **Export** button or select **Export Selected** from the **Actions** menu.

5. In the **Export Entities** screen, click **Export**.

6. In the **Save** screen, click **OK**.

## 20.8 Importing Entities

To import entities:

1. Navigate to the **Entities Search** page, as described in Section 20.2, "Navigating to the Entities Search Page."

2. In the **Entities Search** page, click **Import**.

3. In the **Entities Import** screen, click **Browse** and locate the entity file you want to import.

4. Click **OK**.

## 20.9 Activating Entities

To activate entities:

1. Navigate to the **Entities Search** page, as described in Section 20.2, "Navigating to the Entities Search Page."

2. In the **Entities Search** page, enter the search criteria you want and click **Search**. Refer to Section 20.3, "Searching for Entities."

3. Select the row for each entity you want to activate.

4. Press the **Activate** button.

   When you press **Activate**, the entity is validated for errors (if data elements are present). If there are any errors, they must be fixed before the entity is activated.

   Only active entities can be used in a transaction. Make sure to activate an entity definition if you want to use it in a transaction.

## 20.10 Deactivating Entities

To deactivate entities:

1.  Navigate to the **Entities Search** page, as described in Section 20.2, "Navigating to the Entities Search Page."

2.  In the **Entities Search** page, enter the search criteria you want and click **Search**. Refer to Section 20.3, "Searching for Entities."

3.  Select the row for each entity you want to deactivate.

4.  Press the **Deactivate** button.

## 20.11 Deleting Entities

To delete entities:

1.  Navigate to the **Entities Search** page, as described in Section 20.2, "Navigating to the Entities Search Page."

2.  In the **Entities Search** page, enter the search criteria you want and click **Search**. Refer to Section 20.3, "Searching for Entities."

3.  Select the row for each entity you want to delete and select the **Delete** button from the toolbar.

    If the entities selected for deletion are not used or linked to a transaction, a warning message is shown asking for confirmation.

    If an entity is used, you will not be allowed to delete it.

4.  Click **Delete** to delete the entities.

5.  In the confirmation dialog, click **Yes**.

When multiple entities are selected for deletion and if there are transactions that contain the instances of some of the entities selected, a warning message is provided, stating "The following instances are linked to transactions and cannot be deleted. Do you want to delete the other entities?" If you click **Delete**, the unlinked entities are deleted.

If you deactivate an entity, it will not be available for you to use in transactions.

## 20.12 Re-ordering the Rows in the ID Scheme and Display tabs

After adding all the elements, you can reorder the columns by dragging and dropping the rows for the **ID scheme** and **Display** tabs. Both in **ID Scheme** and **Display** tabs, order is important.

The order of the rows in the **ID scheme** tab determines how information is stored in database and used uniquely identify.

The order of the rows in the **Display** tab determines the order in which information is presented.

For example, in the display, you may want "City, State, Zip code" for addresses in the UK and USA.

## 20.13 Best Practices

This section outlines some best practices for entity creation.

- Any sensitive data, such as credit card and social security numbers, should be encrypted in the database.

- Do not change the external ID. The external ID references how data is identified in the application.

- In order for Oracle Adaptive Access Manager to perform analysis on transactions, you must determine how to represent the transactions in Oracle Adaptive Access Manager, how to process the data coming in, how to use the data, and how to display the data. For example, in an eCommerce transaction, the data involved are credit card numbers, shipping and billing addresses, names, dollar amounts and so on; for a wire transfer, the data involved are Amount, Name, To account, From account, Routing Number, Bank Address, Bank Phone, and so on. Determining which items in a transaction are entities and creating the entities saves time, improves performance in the system, decreases the amount of data created, and enables rules using the entity to run faster than if they had used transactional data.

  An entity can be used and reused in multiple places, which makes creating transaction definitions much easier. An example of an entity that can be reused is an address. A shipping address and billing address can be created for different transactions from the address entity. If you had defined address as transactional data, you would have to define it twice.

- If you want to rearrange the fields in the database for performance purposes, you can modify the row and column values. Only the first 3 columns out of the ten are indexed by default. Rearranging the fields impacts performance.

# 21

# Managing Transactions

This chapter focuses on the creation of transaction definitions. Information on other procedures will also be provided.

## 21.1 Introduction and Concepts

This section introduces you to the concept of transaction definitions and how they are used in Oracle Adaptive Access Manager.

### 21.1.1 Transactions

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

With each type of transaction, different types of details are involved.

For example, in an online transaction, the data involved may be credit cards, e-checks, debit cards, dollar amounts, name, shipping and billing addresses, and so on.

Oracle Adaptive Access Manager can evaluate the risk associated with a transaction in real-time to prevent fraud and misuse.

An Oracle Adaptive Access Manager transaction defines the structure that application data should be mapped to that will enable effective analytics.

The core elements of an Oracle Adaptive Access Manager transaction are:

- entities
- transaction data

When defining a transaction entities and/or transaction data must be defined.

### 21.1.2 Entities

An **Entity** is a user-defined structure, which comprises of a set of related fields grouped together, that can be re-used across different transactions. An entity is used to model a real object. For example, an "employee" entity will have a name, height, social security attributes. From the employee entity you could create an instance for contractors, offshore employees, and so on.

Figure 21–1 shows an example of the employee entity.

**Figure 21–1 Entity Example**
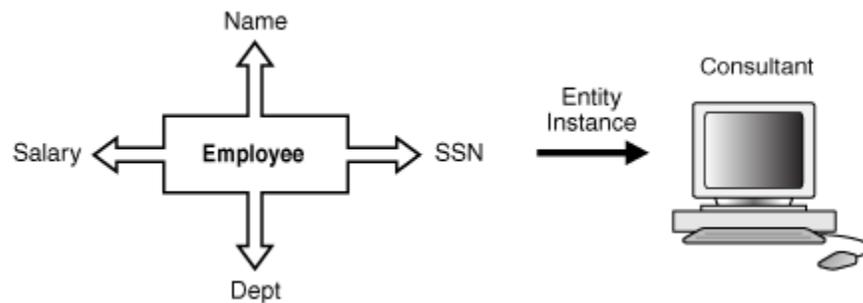


### 21.1.3 Transaction Data

Transaction data is unique for each transaction occurrence and therefore not reusable across different transactions. For example, the total dollar amount of a transaction would not be reused in multiple transactions so it should be transaction data and not an entity.

### 21.1.4 Transaction Handling

You determine the entities and transaction data to use to represent the transactions so that the Oracle Adaptive Access Manager server can process the information from the client application.

## 21.2 Overview of Defining and Using Transaction Definition

In transaction handling, an administrator using Oracle Adaptive Access Manager defines the entities and transaction data to use (transaction definition) to represent the client transactions.

The entities and transaction data elements are then mapped to the source data (client-specific data) so that the Oracle Adaptive Access Manager server can process the information from the client application

To set up transaction definitions:

1. Identify all the entities and transaction elements for the third-party transaction.

   (Determine the fields of interest in the third-party online transaction page.)

   For example, typical fields of interest can be the following:

   - Address
   - Account
   - Credit Card
   - Customer
   - Product Details

2. Create entities for objects in the real world and activate them.

   For example, a home address entity can have StreetNumber, StreetName, AptNumber, City, State, and ZIP.

   For details for creating entities refer to Chapter 20, "Creating and Managing Entities."

**3.** Create a transaction definition. The transaction definition captures the transaction that directly maps with the customers transaction. This definition will be used in policies for monitoring.

*Figure 21–2   Entities and Transaction Data Association with Source Data*
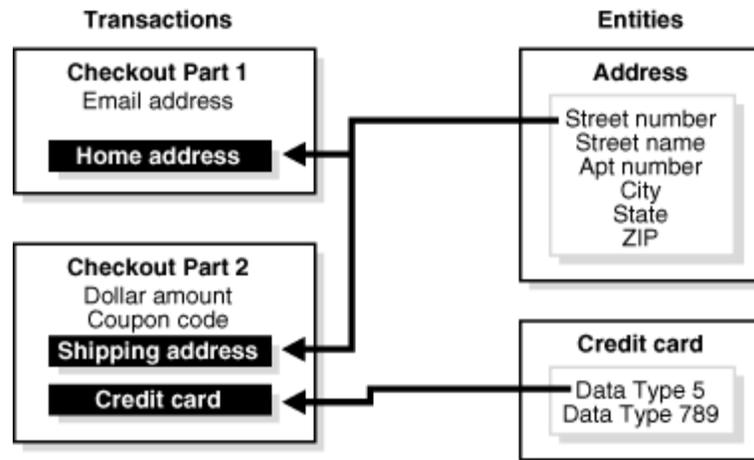


**4.** Add the entities to the transaction definition.

Refer to Section 21.8, "Adding an Existing Entity to the Transaction" or Section 21.9, "Creating a New Entity and Adding It to the Transaction" for details.

**5.** Define transaction data elements for the transaction at the Oracle Adaptive Access Manager End.

For example, Transaction Amount and Transaction Date.

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

Refer to Section 21.10, "Defining Transaction Data for the Transaction at the Oracle Adaptive Access Manager End" for details.

**6.** Define the parameters (source data elements) for the transaction from the client's end.

Source data elements are a list of parameters from the client's end. Details from the external application fill in these fields. Make sure the source data internal IDs match to the keys used by the external application while sending the transaction data.

Refer to Section 21.11, "Defining Parameters for the Transaction from the Client's End" for details.

**7.** Map source data to transaction data and entities.

Refer to Section 21.12.2, "Mapping Entities to the Source Data" for details.

**8.** Activate the transaction definition.

Refer to Section 21.17, "Activating a Transaction Definition" for details.

*Figure 21–3   Source Mapping to Transaction Data and Entities*
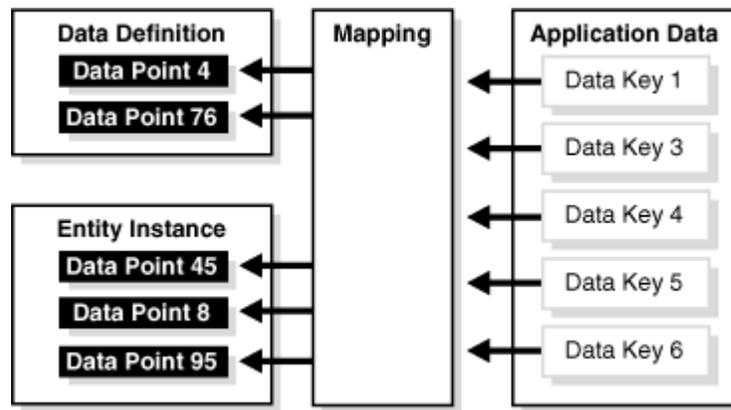


9.  Create an alert. The alert is used to notify administrators about anomalies or send information about the system when rules are triggered.

10. Create a policy that uses transaction conditions.

11. Add a rule to the policy. The rule must contain a transaction condition.

12. When adding the rule to the policy, select your transaction definition for the **Select Transaction to check** field.

13. Link the alert to the policy.

14. Verify the policy by logging into the client application and performing transactions.

## 21.3  Navigating to the Transactions Search Page

The Transaction Search page is the starting place for managing your transaction definitions.

To open the Transactions Search page, click **Transactions** in the Navigation tree.

You could also open the Transactions Search page by right-clicking **Transactions**.

Alternatively, you can:

■   Right-click **Transactions** in the Navigation tree and select **List Transactions** from the context menu.

■   Select **Transactions** in the Navigation tree and then choose **List Transactions** from the **Actions** menu.

■   Click the **List Transactions** button in the Navigation tree toolbar.

From the Transactions Search page, you can:

■   Search for transaction definitions

■   View transaction definitions

■   Create new transaction definitions

■   Activate transaction definitions

■   Deactivate transaction definitions

■   Import transaction definitions

■ Export transaction definitions

The bulk action cannot be selected for creating new, activating, and deactivating transaction definitions.

## 21.4 Searching for a Transaction Definition

On the Transactions Search page you can view a list of all transaction definitions and search for a transaction definition based on various criteria. The Transactions Search page provides access to the Transaction Details page for any transaction.

To search for a transaction definition:

1. Navigate to the **Transactions Search** page, as described in Section 21.4, "Searching for a Transaction Definition."

2. Specify criteria in the Search Filter to locate the transaction and click **Search**.

   The search filter criteria are described in Table 21–1, " Search Filter Criteria".

   If you want to reset the search parameters to the default setting, use the **Reset** button.

*Table 21–1    Search Filter Criteria*

| Field | Description |
| --- | --- |
| Name | The name of the transaction |
| Key | This Key value that is used to map the client/external transaction data to transactions in the Oracle Adaptive Access Manager server. |
| Keyword | The keyword. The keyword filter may increase the likelihood of meaningful search results. |
| Status | The status of the transaction |

The **Search Results** table displays a summary of the transactions that match these criteria specified.

By default, transactions are sorted on **Name**, but you can sort transactions on **Key**, and **Keyword**.

Each transaction has a name. If the description is too long to be fully shown, you can place the mouse over the text to see the entire description.

## 21.5 Viewing Transaction Definitions

The **Search Results** table displays a summary of the transactions that match the search criteria.

Click the row for the transaction you are interested in to view more details.

## 21.6 Prerequisites for Using Transactions

The prerequisites for using Transactions is as follows:

1. Using the Transactions feature involves native integration. The client's transaction page is used to pass the required information to Oracle Adaptive Access Manager to monitor the activity.

2. Transaction data is saved into the Oracle Adaptive Access Manager Server using the APIs described in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

3. Only appropriate and related fields should be grouped into an entity.

## 21.7 Creating the Transaction Definition

To start the creation of the transaction definition:

1. In the **Transactions Search** page, click the **New Transaction** button.

   A **New Transaction Definition** screen appears.

   Alternatively, you can:

   - Right-click **Transactions** in the Navigation tree and select **New Transaction** from the context menu.

   - Select **Transactions** in the Navigation tree and then choose **New Transaction** from the **Actions** menu.

   - Click the **Create new Transaction** button in the Navigation tree toolbar.

   - Select the **Create New Transaction** button from the **Search Results** toolbar.

   - Select **New Transaction** from the **Actions** menu in **Search Results**.

2. In the **New Transaction Definition** screen, enter the transaction definition name.

   Enter a valid name for the name. It must be unique. Transaction definition names are not case-sensitive.

3. Enter the description.

   Enter a description of the transaction definition to be used for informational purposes only.

4. Enter the definition key.

   This definition key value is used to map the client/external transaction data to transaction definitions in Oracle Adaptive Access Manager.

   This value is sent while making the API call for creating or updating the transaction data in OAAM Server.

5. After making the required entries, click the **Apply** button.

## 21.8 Adding an Existing Entity to the Transaction

In the **Entity Selection** page:

1. Click **Add Existing Entity**.

   The **Add Entity** screen appears.

2. Search for the entity and click **Next**.

   Inactive entities are not available for adding to transactions.

   You can single-select an entity.

3. Enter the instance name.

   The instance name must be unique. You can edit the instance name at a later date if needed.

4. Click **Add**.

   The **Edit Entity** screen appears.

5. In the **Edit Entity** screen, you can change the instance name and display order. Then click **Save**.

6. Perform Steps 1 through 5 to add additional existing entities.

You can add multiple instances of the same entity.

The display order is autogenerated and takes the next available order. You can change the order if needed later on.

## 21.9  Creating a New Entity and Adding It to the Transaction

In the **Entity Selection** page:

1. Click **Create New Entity**.

2. Enter **Entity Name** and **Description** and click **Next**.

   Refer to Section 20.4.1, "Initial Steps" in Chapter 20, "Creating and Managing Entities" for details.

3. In the **Entity Data** page, add data elements of the entity.

   Refer to Section 20.4.2, "Adding and Editing Data Elements" in Chapter 21, "Managing Transactions" for details.

4. In the **Entity ID Scheme** page, select the elements that you want to use to uniquely identify an entity.

   Refer to Section 20.4.3, "Selecting Elements for the ID Scheme" in Chapter 20, "Creating and Managing Entities" for details.

5. In the **Entity Display** page, specify the data elements to present and their order when you display the value of the entity and click **Finish**.

   **When the entity is saved, you are taken back to the transaction data screen.**

   You can cancel entity creation by using the **Cancel** button. The **Entity Selection** screen will appear when you press **Cancel**.

   Refer to Section 20.4.4, "Specifying Data for the Display Scheme" in Chapter 20, "Creating and Managing Entities" for details.

6. Perform Steps 1 through 5 to create new entities to add to the transaction definition.

## 21.10  Defining Transaction Data for the Transaction at the Oracle Adaptive Access Manager End

To add transaction data to the transaction definition, follow these steps.

1. In the **Transaction Data** page, click **Add Row**.

2. Enter the data name.

3. Enter the data type.

4. Enter the internal ID.

The internal ID is used to identify the data element. The internal ID specified in the transaction data will be for internal use. It is typically used in rule conditions and other purposes. Do not change this internal ID after it is defined.

5. Enter a description.

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 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."

8. Click **Add**.

9. Add other elements by following Steps 2 through 8.

   You must fill in the required fields for the previous row before you add new transaction data to the transaction definition.

10. Press the **Next** button to add source data.

### Row and Column Values

Row and column values are automatically assigned by the Oracle Adaptive Access Manager Server. If there is a need to change the Row and Column values, follow these guidelines:

1. 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.

2. For a given row there can be a total of 13 fields.

3. For Non-Numeric fields, Column value should be 1 to 10.

4. 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.

## 21.11 Defining Parameters for the Transaction from the Client's End

The source data is defined by the client. To add source data elements to the transaction definition, follow these steps:

1. In the **Source Data** page, click **Add Row**.

2. Enter the data name.

   The data name provides a way to identify the element.

   The data name must be unique.

3. Enter the data type.

4. Enter the internal ID.

   The client supplies the internal ID.

5. Enter a description.

6. Specify whether the source data is needed.

7. Press **Add**.

8. Add other elements by following Steps 1 through 7.

9. After adding all the source data elements, click **Next**.

## 21.12 Mapping the Source Data

Mapping is a way to connect the source data to transaction data and to entities.

### 21.12.1 Mapping Transaction Data to the Source Data

To connect the transaction data to the source data:

1. In the **Data Mapping** section of the **Mapping** page, click **Map Data**.

2. Select the transaction data.

   The data elements to choose from are the ones you defined in the "Defining Transaction Data for the Transaction at the Oracle Adaptive Access Manager End" section.

3. Select the **Source Data**.

   The client data elements to choose from are the ones that you added in the "Defining Parameters for the Transaction from the Client's End" section.

4. Select the mapping type.

   Select **Direct**, **Concatenate**, **Endstring**, and **Substring**.

   - Select **Direct** if you want a one-to-one mapping of the source data element to the destination data element.

   - Select **Concatenate** if you want to join two or more source data elements to form one data element.

   - Select **Endstring** if you want to have last "x" number of characters from source data as the data.

   - Select **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 **Map**.

8. Map other elements by following Steps 2 through 6.

9. Click **Finish** or perform mapping for entities.

## 21.12.2 Mapping Entities to the Source Data

To add the mapping for the Entity elements, follow these steps:

1. In the **Entities Mapping** section of the **Mapping** page, click **Map Entity**.

2. Select the entity.

3. Select **Source Data**.

4. Select the mapping type.

   Select **Direct**, **Concatenate**, **Endstring**, and **Substring**.

   ■ Select **Direct** if you want a one-to-one mapping of the source data element to the destination data element.

   ■ Select **Concatenate** if you want to join two or more source data elements to form one data element.

   ■ Select **Endstring** if you want to have last "x" number of characters from source data as the data.

   ■ Select **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. Click **Map**.

8. Click **Finish** or perform mapping for transaction data.

   When the transaction definition is created, the new **Transaction Details** page opens.

## 21.12.3 Editing Mapping

For transaction data, you can specify the transaction data, source data, and mapping type.

For entity mapping, you can specify the entity name, transaction data, source data, and mapping type.

## 21.13 Activating the Transaction Definition

By default, a transaction definition is disabled on create.

Activate the transaction definition using the **Activate** button in the **Transaction Details** page.

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

## 21.14 Editing a Transaction Definition

To edit the details of a specific transaction definition, follow these instructions:

When modifying transaction definitions, do not change the Definition ID. The Definition ID may be referenced by other applications.

1. If you are not on the **Transaction Definition Details** page of the transaction definition you want to edit, follow the instructions in Searching for a Transaction Definition.

2. In the **General** tab, to edit the transaction definition name and description.

3. In the **Entity** tab, select the entity you want, click **Edit Entity**, and edit the entity.

4. In the **Data** tab, edit the data elements.

5. In the **Source Data** tab, perform edits.

6. In the **Mapping** tab's **Data Mapping** section, click **Edit Mapping**, and edit the source data and mapping type and click **Map**.

7. In the **Mapping** tab's **Entity Mapping** section, click **Edit Mapping**, and edit the entity name, transaction data, source data, and mapping type fields.

8. Click **Apply** or **Revert**.

   If you click **Apply**, transaction definition updates are applied.

   If you click **Revert**, transaction definition updates are not applied

## 21.15 Exporting Transaction Definitions

To export transaction definitions:

1. Navigate to the **Transaction Definitions Search** page, as described in Section 21.3, "Navigating to the Transactions Search Page."

2. In the **Transaction Definitions Search** page, enter the search criteria you want and click **Search**. Refer to Section 21.4, "Searching for a Transaction Definition."

3. Select all the rows corresponding to the transaction definitions you want to export.

4. Click the **Export** button or select **Export Transaction Definition** or **Generate Delete Script** from the **Actions** menu.

5. In the **Export Transaction Definition** screen, click **Export**.

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

6. Save the file to disk.

   The file is exported.

7. Click **OK**

If the transaction definition selected for export and deletion is not used or does not contain transaction data from the past, a confirmation dialog is shown asking for a confirmation. If you answer "yes", the transaction definition is deleted.

When multiple transaction definitions are selected for export and deletion and if some of the transaction definitions are used or contain transaction data from the past, a message appears, telling you which ones can be deleted and which ones cannot be deleted. Links to a usage tree are available for each of the used transaction definitions. In the dialog, you are also given the option to delete the ones that are not in use or contain transaction data from the past.

## 21.16 Importing Transaction Definition

To import a transaction definition:

1. Navigate to the **Transaction Definitions Search** page, as described in Section 21.3, "Navigating to the Transactions Search Page."

2. In the **Transaction Definitions Search** page, click **Import** or select **Import Transaction Definition** from the **Actions** menu.

3. In the **Transaction Definition Import** screen, click **Browse** and locate the transaction definitions you want to import.

4. Click **OK**.

## 21.17 Activating a Transaction Definition

To activate a transaction definition:

1. Navigate to the **Transaction Definitions Search** page, as described in Section 21.3, "Navigating to the Transactions Search Page."

2. In the **Transaction Definitions Search** page, enter the search criteria you want and click **Search**. Refer to Section 21.4, "Searching for a Transaction Definition."

3. Select the row corresponding to the transaction definition you want to activate.

4. Press the **Activate** button or select **Activate** from the **Actions** menu.

The **Activate** button is disabled if multiple rows are selected.

All the required information must be entered (in all tabs), before you can activate the transaction. At least one source data element should be present.

## 21.18 Deactivating a Transaction Definition

To deactivate a transaction definition:

1. Navigate to the **Transaction Definitions Search** page, as described in Section 21.3, "Navigating to the Transactions Search Page."

2. In the **Transaction Definitions Search** page, enter the search criteria you want and click **Search**. Refer to Section 21.4, "Searching for a Transaction Definition."

3. Select the row corresponding to the transaction definition you want to deactivate.

4. Press the **Deactivate** button or select **Deactivate** from the **Actions** menu.

The **Deactivate** button is disabled if multiple rows are selected.

## 21.19 Deleting Transaction Definitions

To delete transaction definitions:

1. Search for the transaction definition you are interested in, as described in Section 21.4, "Searching for a Transaction Definition."

2. Select the row corresponding to the policies you want to delete and press the **Delete** button or select **Delete Transaction Definition** from the **Actions** menu.

   A warning message reminds you that the changes will be permanent and asks if you want to continue.

   If the transaction definitions selected for deletion are not actively used or contain transaction data from the past, a confirmation message is shown asking for confirmation. If you answer "yes", those transaction definitions are deleted.

3. In the Information dialog, click **OK**.

If you have a transaction definition and it has transaction data from the past or is being used, you are not allowed to delete the definition.

When multiple transaction definitions are selected for deletion and if some of the transaction definitions are used or contain transaction data from the past, a warning message appears, stating: "The following instances are used and cannot be deleted. Do you want to delete the other transaction definitions?" If you answer "yes", the unused transaction definitions are deleted.

## 21.20 Use Cases

This section describes example use cases for using transaction definitions.

### 21.20.1 Implementing a Transaction Use Case

Joe is a retail banking customer. Retail banking customers can make money transfers totaling up to $500 per day.

Implementation Tasks:

1. Identify the source data fields that make up the **Money Transfer** transaction.

2. Give a unique identifier that identifies the transaction type of **Money Transfer**.

3. Determine how to model the **Money Transfer** transaction in OAAM in terms of OAAM entities and transactions.

   Refer to Section 21.1, "Introduction and Concepts" to find out what can be modeled as a transaction and an entity.

4. Identify the mapping between the source data of **Money Transfer** and OAAM entities and transaction.

5. Use OAAM Admin to create and activate the entities and transaction definitions for **Money Transfer** based on the model you came up with.

6. Determine the OAAM checkpoint that can be used to trigger the fraud policies that can perform fraud checks on the **Money Transfer** transaction. If an existing checkpoint can be reused, there is no need to create a checkpoint. Otherwise, create an OAAM checkpoint for the **Money Transfer** transaction.

7. Now, look at the requirements for what kind of rules should go into the fraud policy for this transaction.

8. Based on the use case, you would want to enforce a threshold on the total in money transfer allowed per day.

9. Look at the list of transaction rule conditions in Section C.2.6, "Transactions Conditions." Go through the "Possible User Scenarios" section of those rule conditions.

10. For this use case, the rule condition "Transaction: Check Transaction Aggregrate and Count Using Filter Conditions" can be used to check if the user has reached the threshold of $500 in money transfer per day.

11. Create an OAAM policy and add the rule using the "Transaction: Check Transaction Aggregate and Count Using Filter Conditions" rule condition and specify the following in the rule condition:

*Table 21–2   Transaction Rule Configuration*

| Parameters | Values |
| --- | --- |
| Transaction to check | Choose the transaction definition of Money Transfer |
| Aggregrate Function | Sum |
| Entity or Element to count | Select the data field that indicates the "money transfer amount" |
| Condition for Aggregrate | Select "Greater Than Equals" |
| Check value for Aggregrate | 500 |
| Condition for Count | Greater than Equals |
| Check Value for Count | 1 (since you want at least 1 transaction to be there) |
| Duration | 1 rolling day (if last 24 hours to be treated as a day) or 1 Calendar day (if the current calendar day i.e. 12am to 11.59 pm has to be considered) |
| Transaction Status | Select if only transactions in a particular status have to be considered |
| Ignore Current Transaction in Count | Select TRUE if current transaction should be excluded. If it is has to be included select FALSE and make sure the transaction data is created before running the rules. |
| For the same User? | Default is TRUE which makes sense since you want to consider only the transactions of current user |
| Apply filter checks on Current Transaction | Select TRUE if there are any conditions in Query Filter and you want to apply them to current transaction first |
| Query Filter | Select any filters so that you can fine tune what transactions have to be chosen to compute the aggregate before it checks if the threshold is reached. |

12. Once the rule condition is configured, specify what should be the **Results** if the rule condition is satisfied. You can configure **Alert** and **Action** groups that indicate that the user has reached his threshold and also a **score**. The client application can interpret the result and take appropriate action in terms of redirecting the user to the relevant pages that indicate that the user action is not allowed.

13. Now, you have the setup ready in OAAM so that the transaction can be created in OAAM and fraud policies and rules can be triggered.

14. Integrate the client application with OAAM using OAAM shared libraries. Refer to "Integrating Native Java Applications" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager* for details of the integration. This is required since transactions functionality is available through native integration. As part of this integration, the client application does two things:

- Call the OAAM Data Collection API to pass the transaction data. OAAM Data Collection APIs persist the transaction data based on the transaction definition into the OAAM database. This results in the creation of OAAM entities and transaction data. The output of these APIs is a Transaction ID.

- Call the OAAM Rules API to trigger the fraud policies/rules associated to the checkpoint. This step results in triggering the rules engine that would execute the policies and rules associated to this checkpoint and creating Alerts if the associated rules trigger. The output of these APIs is a set of actions and risk score as returned by the policies and rules.

15. Once the integration with client application is done, you can perform a sample money transfer transaction and verify the end-to-end flow.

## 21.20.2 Use Case: Transaction Frequency Checks

These kinds of checks can be implemented using the "Transaction: Check Transaction Count Using Filter Condition" rule condition. Table 21–3 shows the important parameters of the rule condition.

*Table 21–3    Transaction Frequency Checks*

| Parameters | Values |
| --- | --- |
| Select Transaction to count | Select the transaction definition for which this check has to be applied |
| Specified Condition For Count | Select "Greater Than Equals" |
| Specified Check Value for Count | Enter the frequency value |
| Duration | Enter the duration |

## 21.20.3 Use Case: Transaction Frequency and Amount Check against Suspicious Beneficiary Accounts

This kind of check can be implemented using the "Transaction: Check Transaction Aggregrate and Count Using Filter Conditions" rule condition. Table 21–4 shows the important parameters of this rule condition.

*Table 21–4    Transaction Frequency and Amount Check against Suspicious Beneficiary Accounts*

| Parameters | Values |
| --- | --- |
| Select Transaction to check | Select the transaction definition for which this check has to be applied |
| Select Aggregrate Function | Sum |
| Select Entity or Element to count | Select the numeric data field that indicates the "amount" |
| Select Condition for Aggregate | Select "Greater Than Equals" |
| Specified Check value for Aggregrate | Enter the value of amount to check |
| Specified Condition for Count | Greater than Equals |
| "Specified Check Value for Count | Enter frequency value |
| Duration | Enter the duration |

## 21.20.4 Use Case: Transaction Check against Blacklisted Deposit and Beneficiary Accounts

This kind of check can be implemented using the "Transaction: Check Current Transaction Using Filter Condition" rule condition.

Before configuring the rule, create the two groups of accounts, one that has the list of blacklisted deposit accounts and the other that has the list of blacklisted beneficiary accounts. Those groups should be populated with the lists of accounts that are blacklisted. These tasks can be done using OAAM Admin.

After that, create the rule using the "Transaction: Check Current Transaction Using Filter Condition" rule condition and configure it as follows:

***Table 21–5    Transaction Check against Blacklisted Deposit and Beneficiary Accounts***

| Parameters | Values |
| --- | --- |
| Select Transaction to check | Select the transaction definition for which this check has to be applied |
| Filter condition | Select Deposit Account Data Field from the Transaction and specify the condition as "IN" and then select the group as the Blacklisted Deposit Accounts |
| Filter condition | Select Beneficiary Account Data Field from the Transaction and specify the condition as "IN" and then select the group as the Blacklisted Beneficiary Accounts |

## 21.20.5  Use Case: Transaction Pattern

Example: Configure a rule to find out whether several small transactions (where amount < $10) has happened before a big transaction (amount > $500) is attempted in the last couple of hours. If yes, then the user should be challenged before this huge transaction.

To configure this kind of check the rule condition "Transaction: Check if consecutive Transactions in given duration satisfy the filter conditions" can be used.

The rule condition parameters have to be configured as follows:

***Table 21–6    Transaction Pattern***

| Parameters | Values |
| --- | --- |
| Select Transaction to check | Select the transaction definition for which this check has to be applied |
| Duration | Enter the duration of transactions that has to be considered |
| Allow gaps in transactions during checks? | If gaps are allowed then select TRUE, otherwise select FALSE |
| No of transactions to check for 1st set of conditions | Enter number of transactions that should match the first set of conditions. For example, if you want to first check 2 small transactions then enter the value as "2". |
| Checks for 1st set of conditions | Enter the following conditions that should match the first set of transactions<br><br>■   Select Amount data element with condition as "Less Than" and value as 10. |
| No of transactions to check for 2nd set of conditions | Enter number of transactions that should match the first set of conditions. For example, if you want to check 1 big transaction after 2 small transactions then enter the value for "No of transactions to check for 2nd set of conditions" as "1". |
| Checks for 2nd set of conditions | Enter the following condition that should match the next set of transactions.<br><br>■   Select Amount data element with condition as "Greater Than" and value as 500 |

### 21.20.6 Use Case: Composite or Nested Transactions

A composite transaction is when a master transaction is defined, and then a child transaction is defined, and the child transaction is associated with the parent.

Composite or Nested Transactions can be implemented in OAAM by performing the following tasks:

1.  Identify the master/parent transaction and the detail/child transaction.

2.  Identify the data element that uniquely identifies the master/parent transaction; add that data element as one of the transaction data elements to the detail/child transaction definition.

3.  Configure two different checkpoints. One checkpoint for evaluating fraud policies on master/parent transaction and the other for evaluating fraud policies on detail/child transactions.

4.  Make sure the client application makes separate OAAM Data Collection API calls to persist the transactions of master/parent transaction the detail/child transactions.

5.  Policies related to detail/child transactions can be evaluated first to see if there are suspicious child transactions. To consider other child transactions that are part of the same parent transaction, the parent transaction identifier can be used since that is the common data element that ties all the child transactions together.

Currently there are no specific rule conditions that act on composite transactions.

# Part VII

## OAAM Offline Environment

This part contains instructions on how to use an OAAM Offline environment.

# 22

# OAAM Offline

OAAM supports two types of deployment:

- OAAM online can be used to perform real-time risk evaluations
- OAAM offline can be used to perform risk evaluations on historical or non-real time login/transactional data

This chapter provides information about setting up OAAM Offline for rule evaluation and fraud detection.

## 22.1 Concepts

This section provides a brief introduction to OAAM Offline and contains the following sections:

- What is OAAM Offline?
- OAAM Offline Architecture
- OAAM Offline User Interface
- Dashboard Differences

### 22.1.1 What is OAAM Offline?

OAAM Offline can be used for the following purposes:

- Standalone security tool

  OAAM Offline can be used to analyze transactions and logins. Users who do not have an OAAM production system could use an offline system as their primary risk analysis system.

- Research and development tool

  OAAM Offline can be used to create and verify new policies and rules using non real-time customer data without impacting customers in the real-time environment. Users are able to run complicated rules that would take too long to execute in a production system on a secondary system. They run simpler rules in OAAM and use OAAM Offline as the secondary system.

- Supplemental offline analysis tool

  OAAM Offline can be used in the tuning of rules and verification of rules behavior against customer and transaction data without impacting customers in real-time environment.

## 22.1.2 OAAM Offline Architecture

OAAM Offline is a standalone application.Unlike OAAM Online, OAAM Offline does not involve a client application. The relationship between the source data, the loaders, the Web server that hosts OAAM Offline, and the database that stores the customer login and transaction data is shown in Figure 22–1, "OAAM Offline Architecture".

*Figure 22–1    OAAM Offline Architecture*
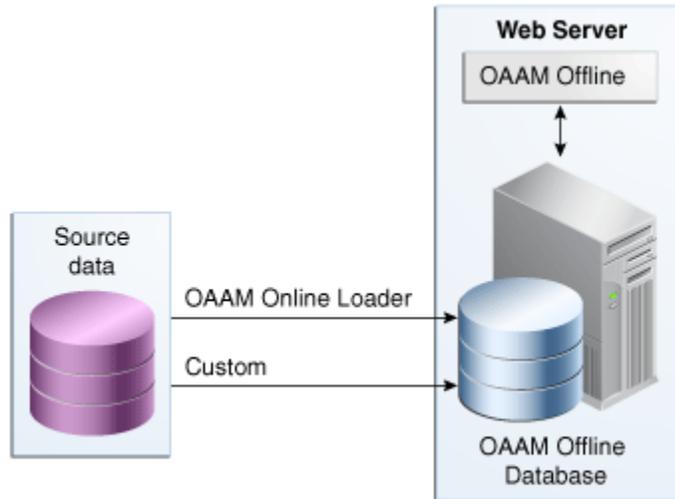


OAAM Offline has its own database. This database has an identical schema to that of the OAAM Online version. It is used to load customer data to perform risk analysis and tune rules. OAAM Offline can support both login and transaction data. For information on the types of loaders that are used to load data, refer to Section 22.1.7, "Data Loaders."

If you want to load the customer data (source data) into the Offline database, you will need to create a Load Job, and a data loader is required to load the data into the database.

## 22.1.3 Jobs

A job is a collection of tasks that can be run by OAAM. You can perform a variety of jobs such as load data, run risk evaluation, roll up monitor data, and so on. Out of the box, OAAM supports the following jobs:

*Table 22–1    Jobs*

| Jobs | Descriptions |
| --- | --- |
| Load | A Load Job reads records from a remote data source, converts the data into OAAM login sessions, and stores the login sessions in the OAAM offline datastore. |

*Table 22–1   (Cont.)  Jobs*

| Jobs | Descriptions |
| --- | --- |
| Run | A Run Job performs risk analysis on a set of OAAM sessions. When a Run starts execution, it performs a clean up for the records in the Job's data filter. This clean up involves deleting rule logs, alerts, and actions and resetting risk scores and authentication statuses. |
| Load and Run | A Load and Run Job is a combination of a Load Job and a Run Job. After each record is processed by the Load Job, the result is fed directly into the Run Job. |
| Monitor Data Rollup | A Monitor Data Rollup Job consolidates monitor data utilized in the dashboard and some risk evaluations on a regular basis. This job consolidates data to optimize the database when processed. |

Users can schedule jobs and run them offline. For information on jobs, refer to Chapter 23, "Scheduling and Processing Jobs in OAAM."

## 22.1.4  What is a Load Job and How Do You Set One Up

A Load Job reads records from a remote data source, converts the data into OAAM login sessions, and stores the login sessions in the OAAM offline datastore.

The process for creating a Load Job is as follows:

1.  Specify the type of loader to use to load the data into the Offline database and the database connection details. If you are using the OAAM loader, the mapping details of the remote database to the OAAM schema is already provided, but you can edit these on the database-side if necessary.

2.  Specify a data filter to define the set of records in the database to be loaded.

3.  Set up the scheduling for when to run the Load Job.

A Load Job begins by connecting to the database defined in the Job's connection properties, and executes a SQL Query constructed from the Job's data mapping properties and filtered by the values in the Job's Data Filter. It then takes the results from that query and generates login records in the OAAM Offline database. As it generates the logins, it also runs the device identification checkpoint so that cookies are assigned. For information on creating a Load Job, refer to Section 23.4.1, "Creating Load Jobs," and for information on data loaders, refer to Section 22.1.7, "Data Loaders,"

## 22.1.5  What is a Run Job and How Do You Set One Up?

A Run Job performs risk analysis on a set of OAAM sessions.

The process for creating a Run Job is:

1.  Define how and under what conditions the OAAM policies are applied to the sessions.

2.  Set up the data filter to define the set of records in the database to be loaded or run.

3.  Set up the scheduling for when to run the Run Job.

When a Run starts execution, it performs a clean up for the records in the Job's data filter. This clean up involves deleting rule logs, alerts, and actions and resetting risk scores and authentication statuses. The Run Job is executed based on the Run Type. For information on creating Run Jobs, refer to Section 23.4.2, "Creating Run Jobs,"

## 22.1.6  Load and Run Job

A Load and Run Job is a combination of a Load Job and a Run Job. After each record is processed by the Load Job, the result is fed directly into the Run Job.

## 22.1.7  Data Loaders

Loaders load the customer login or transaction data that will be processed for jobs.

*Figure 22–2   Data Loaders*
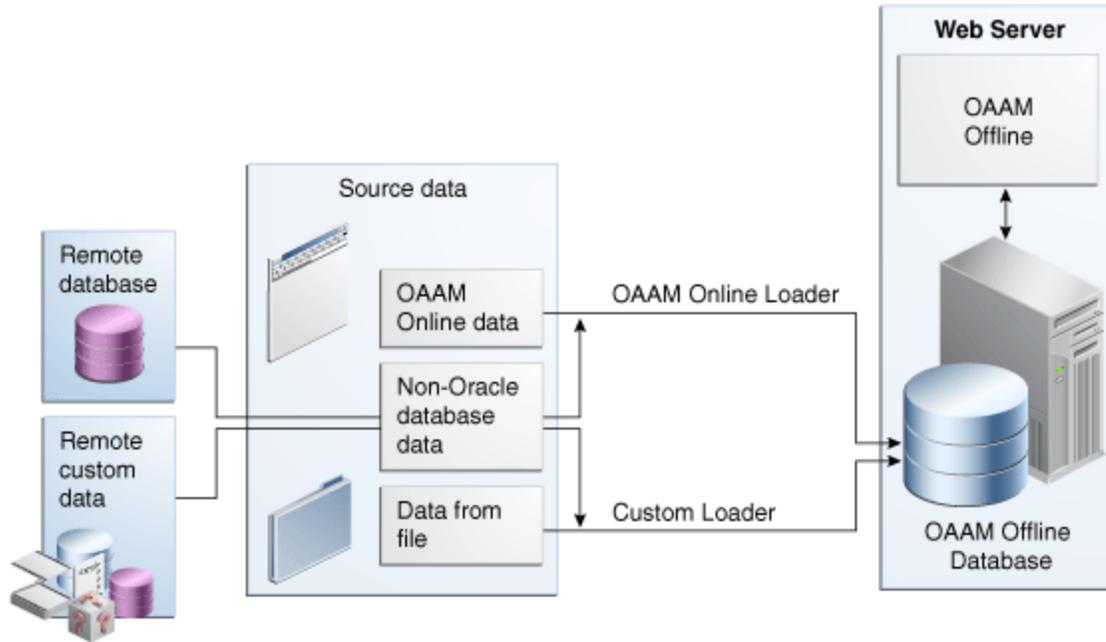


The standard OAAM Loader, which is shipped with OAAM, can be used to load login data from an OAAM schema database or a remote database that is mapped to the OAAM schema.

Custom data loaders are developed to accomplish complex and custom use cases specific to a deployment. Login and transaction data can be loaded from almost any source including files. OAAM supports custom loaders. For more information on developing a custom loader, refer to the "*Developing a Custom Loader for OAAM Offline*" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

Table 22–2 summarizes the differences between the default and custom loaders.

*Table 22–2    OAAM Loader vs. Custom Loader*

| Loaders | Shipped With OAAM | Loads any data | Loads from any source | Complex data mapping | Use case |
|---------|-------------------|----------------|------------------------|----------------------|----------|
| OAAM Loader | Yes.<br><br>Default loader | No<br><br>Loads login data | No<br><br>Loads from an OAAM schema database or a remote database that is mapped to the OAAM schema | No<br><br>Data mapping must be simple and straight forward | Use Case: Configure a Solution to Run Risk Evaluations Offline |
| Custom Loader | No.<br><br>Custom development<br><br>For information, refer to Developing a Custom Loader in the Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager. | Yes<br><br>Loads login and transaction data | Yes<br><br>Loads from remote, custom source including files | Yes<br><br>Used if the data cannot be mapped easily and requires complex SQL queries or some manipulations | Use Case: Load Transactional Data and Run Risk Evaluations from Multiple Sources |

## 22.1.8  Run Type

The Run type defines how and under what conditions the OAAM policies are applied to the sessions. A Run Job using the OAAM Run type reads the set of session records from the database. Pre-authentication checkpoints are run for all sessions in the set. Post-authentication checkpoints are run only for sessions where the user is successfully authenticated.

If you need to change the checkpoints to run, refer to Section 22.10, "Changing the Checkpoints to Run." A Custom Run Job may perform other tasks or run checkpoints differently than our standard checkpoints.

## 22.1.9  OAAM Offline User Interface

The user interfaces of OAAM Online and Offline are identical except for the dashboard and job creation and job monitoring pages.

### 22.1.9.1  Dashboard Differences

The OAAM Offline Dashboard is similar to the OAAM Online Dashboard except for the details listed:

**Uses Non Real-time Customer Data**

The OAAM Offline Dashboard uses non real-time customer data from OAAM Online or from a remote, custom source instead of real-time data.

**Risk Analysis Dashboard**

The OAAM Offline Dashboard provides access to the "Risk Analysis" dashboard, which shows the progress of the current load or run task.

### 22.1.9.2  Job Interface for Load, Run, and Load and Run

The Jobs search page enables you to search for jobs to display and view their details. The Job Creation wizard provides a step-by-step guide through the job definition and scheduling process for Load, Run, and Load and Run Jobs. These jobs are not available in OAAM Online.

### 22.1.9.3  Job Queue

The Job Queue page displays the job instance currently processing and progress in terms of estimated completion time and percentage complete progress. You can cancel or pause and resume a job instance processing from the queue interface. If a job is not set to process via scheduling it will not appear in the Job Queue.

## 22.2  Access Control

Access permissions for the offline environment is detailed in the following table.

*Table 22–3    Offline Environment*

| Role | Access |
|------|--------|
| CSR and CSR Managers | No access |
| Fraud investigators and Investigation Managers | Same access as online including security dashboard |
| System Administrators | Same access as online (Environment node) and full access to scheduler node |
| Security Administrator | Same access as online except the Environment node and full access to scheduler node |

## 22.3  Installation and Configuration of OAAM Offline System

This section describes the steps to configure OAAM Offline.

### 22.3.1  Overview

Table 22–4 presents a summary of the tasks for configuring OAAM Offline. The table also provides information on where to get more details about each task.

*Table 22–4    Tasks in OAAM Offline Setup*

| Task | Description | Documentation |
|------|-------------|---------------|
| Task 1 - Install OAAM offline | OAAM offline installation is similar to the OAAM online installation. | Refer to Section 22.3.2, "Install OAAM Offline." |
| Task 2 - Create the offline database schema | OAAM Offline has its own database. This offline database has an identical schema to that of the OAAM Online version. | Refer to Section 22.3.3, "Create the Offline Database Schema." |

**Table 22–4   (Cont.)  Tasks in OAAM Offline Setup**

| Task | Description | Documentation |
| --- | --- | --- |
| Task 3 - Configure database connectivity | When you configure OAAM Offline with the Oracle Fusion Middleware Configuration Wizard, you will be able to set values for the Schema Owner, Schema Password, Database and Service, Host Name, and Port | Refer to Section 22.3.4, "Configure Database Connectivity." |
| Task 4 - Log in to OAAM Offline | Log in to OAAM Offline. | Refer to Section 22.3.5, "Log In to OAAM Offline." |
| Task 5 - Set up the environment | After installing and configuring OAAM Offline, you must set up the base environment. | Refer to Section 22.3.6, "Environment Set Up." |

## 22.3.2  Install OAAM Offline

Oracle Adaptive Access Manager (Offline) is included in the Oracle Identity and Access Management Suite. You can use the Oracle Identity and Access Management 11*g* Installer to install OAAM Offline.

## 22.3.3  Create the Offline Database Schema

You must create and load the OAAM offline schema before installing OAAM offline. For OAAM, Oracle recommends the Oracle Database Enterprise Edition for production deployments although the Standard Edition can be used as well. You create and load the schema using the Oracle Fusion Middleware Repository Creation Utility (RCU), which is available on the Oracle Technology Network (OTN) Web site. You can access the OTN web site at:

http://www.oracle.com/technetwork/index.html

Later, you will load customer login and/or transaction data into the OAAM Offline database, and OAAM Offline will use this database to perform risk analysis. The following sections provide best practices for the OAAM Offline database.

## 22.3.4  Configure Database Connectivity

When you configure OAAM Offline with the Oracle Fusion Middleware Configuration Wizard, you will be able to set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. You will also be able to test the connectivity.

## 22.3.5  Log In to OAAM Offline

To sign in to OAAM Offline, follow these steps:

1.  In a browser window, enter the URL to the **Oracle Adaptive Access Manager Offline 11g Sign In** page.

    http://*host*:*port*/oaam_offline/

    where

    -   *host* refers to the Oracle Adaptive Access Manager Offline managed server host

    -   *port* refers to the OAAM Admin Offline managed server port

    -   /oaam_offline/ refers to the OAAM Offline Admin Sign In page

**2.** On the **Sign In** page, enter your credentials.

**3.** Click the **Sign In** button.

## 22.3.6 Environment Set Up

After installing and configuring OAAM Offline, you must complete the following tasks to set up the base environment:

- Import the Snapshot

- Set Up Encryption and Database Credentials for Oracle Adaptive Access Manager

- Enable Autolearning

- Enable Configurable Actions

- Import IP Location Data

- Importing Transaction Definitions

### 22.3.6.1 Import the Snapshot

Import the snapshot that is used by both OAAM Online and Offline. The use of snapshots online and offline are identical. The **Snapshot** is a zip file that contains the default policies, rules, groups, and any other information that is needed to configure OAAM Offline. The OAAM snapshot file and located in the *MW_HOME/IDM_ ORACLE_HOME*/oaam/init directory. Refer to Chapter 2, "Setting Up the Oracle Adaptive Access Manager Environment for the First Time" for information on loading the snapshot.

### 22.3.6.2 Set Up Encryption and Database Credentials for Oracle Adaptive Access Manager

Encryption is used to protect data within Oracle Adaptive Access Manager from unauthorized access. The process uses methods and a key or keys to encode plain text into a non-readable form. A key is required to decrypt the encrypted information and make it readable again. Authorized persons who possess the key can decrypt information that is encrypted with the same key. For instructions to set up encryption and database credentials for OAAM Offline, refer to Section 2.4, "Setting Up Encryption and Database Credentials for Oracle Adaptive Access Manager,".

### 22.3.6.3 Enable Autolearning

Only testing of patterns is supported with Autolearning. To use Autolearning (pattern analysis):

**1.** Import default entities.

**2.** Import autolearning policies and rules if you are not using the default snapshot. These are required in order to perform the autolearning run on the data.

**3.** 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
```

For more information, refer to Section 17.3, "Before You Begin to Use Autolearning."

**4.** Define and enable patterns.

**5.** Perform load and the run at the same time.

### 22.3.6.4 Enable Configurable Actions

If you want configurable actions enabled in your system, follow this process:

**1.** Enable the configurable action property.

   Set `dynamicactions.enabled` to `true`.

**2.** Make sure the configurable action definitions are configured in the Oracle Adaptive Access Manager database.

   A user can see the list of available configurable actions before adding a new one.

**3.** Determine what configurable actions have to be added to which checkpoint and the preconditions for executing those configurable actions.

**4.** If the existing Configuration Actions are not sufficient, develop and deploy custom ones. See the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager* for details on developing a configurable action.

   Although some configurable actions are provided with the product, you may have to develop custom templates for your particular requirements.

   **a.** Define the custom action template

   **b.** Load the action template

**5.** Associate the configurable actions to the Checkpoint.

For information on enabling configurable actions, refer to Chapter 18, "Managing Configurable Actions."

### 22.3.6.5 Import IP Location Data

IP location data is used by the risk policies framework to determine the risk of fraud associated with a given IP address (location). To be able to determine location of the login or transaction, this data must be uploaded. For information, see Section 29.4, "Importing IP Location Data."

### 22.3.6.6 Importing Transaction Definitions

Transaction definitions define the mappings of OAAM transaction elements to source data (client-specific data) so that OAAM can evaluate the risk associated with a transaction.

Transaction definitions are available from the Oracle Technology Network (OTN). You can access OTN at:

http://www.oracle.com/technology/

## 22.4 Scheduling Jobs

For information on scheduling jobs, refer to Chapter 23, "Scheduling and Processing Jobs in OAAM." The chapter describes how to define, schedule, and run Oracle Adaptive Access Manager batch jobs.

## 22.5 Testing Policies and Rules

OAAM policies/rules for a new deployment or an existing deployment can be tested using OAAM Offline.

### 22.5.1  New Deployment Using OAAM Offline

You can use a combination of OAAM Offline and BIP reports to test the effect of policies and rules on users. To do this:

1. Deploy an offline instance of OAAM to perform batch analysis

2. Configures the OAAM loader or develop your own to load a set of production data into the offline environment to use as the test set.

3. Run policies/rules against the test set of data multiple times to view the impact of policy changes.

For example, in a new deployment, you can load a month of your production data into OAAM and run the base policies to see how many alerts and actions would have been generated if OAAM had been used in production for one month. The BIP reports are useful to gather aggregate values for the rules and outcomes. In the results you will see that as OAAM learns the behaviors, users will generate fewer alerts and actions. If you add any new rules or edit any rule thresholds you can do another run and compare BIP report outcomes to those from the original run.

### 22.5.2  Existing Deployment Using OAAM Offline

If you have OAAM already in production, you can export a set of production data on which to test the effects of policy/rule changes.

1. Set up a scheduled data load to update the offline environment data every 24 hours

2. When the security team wants to add a new rule or edit a rule threshold they can first run 24 hours of data against the current policies in production and run BIP reports exported to XLS.

3. Then the team can make the edits and run a second time on the same data set and run the same BIP reports.

4. Comparing the reports from Run 1 and Run 2 will reflect how the user population was effected by the policy changes. In other words, if the first run generates 100 alerts and the second run generates 125 alerts, the effect of the edits is 25 additional alerts are generated.

You can also license third party tools for further testing options. For example, IntegratID (http://integratid.com/) has the ARM Automator tool which can be used to simulate very specific traffic scenarios on which to test.

For example, if you want to test if a velocity rule will trigger if a user logs in from Los Angeles at 10:24 am PST then logs in from New York City at 10:45 am PST using the same device.

## 22.6  What to Expect in OAAM Offline

### Setting Up Patterns In Autolearning

In online systems, the administrator can set up patterns at any time and the pattern processing starts for the logins after that point. In offline systems, the administrator must set up the properties and the patterns prior to starting the Load Job, so that when the Load Job runs, the patterns processing occurs simultaneously. This is one of the key differences between online and offline systems.

**Running Jobs in Autolearning**

You cannot perform the load and then the run if you want Auto-learning. Only "Load and Run" is supported for pattern processing. Choose Load and Run as the job type when you are creating jobs. A Load and Run Job is a combination of a Load Job and a Run Job. After each record is processed by the Load Job, the result is fed directly into the Run Job. After the Load and Run Job is submitted, you will need to go to the Job Queue and search for the job in order to view its status and other details.

## 22.7 Monitoring OAAM Offline

This section describes how to monitor OAAM Offline using the Dashboard and Server Logs.

### 22.7.1 Using Dashboard to Monitor the Loader Process

The OAAM Offline Dashboard uses non-real time customer data from OAAM 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 "Risk Analysis" dashboard shows the progress of the current load or run task. Risk Analysis statistics are provided for

- load data: the data loaded from OAAM Online or from a remote, custom source

- run data: the data that policies 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.

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 logins 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.

Offline Job data is based on when records were processed, not timestamp.

### 22.7.2 Enable 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=-1
```

### 22.7.3 Database Query Logs for Performance Monitoring

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.

### 22.7.4 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.

### 22.7.5 Database Tuning

You can monitor and tune the performance of the database using tools like Oracle Enterprise Manager.

### 22.7.6 Manageability

Offline uses Oracle Dynamic Monitoring Service (DMS) for performance monitoring. Information about monitoring performance is in Chapter 26, "Monitoring Performance by Using Fusion Middleware Control."

## 22.8 Creating a View for Offline Loader For Non-OAAM Database

Users who want to load from a non-OAAM database will need to create a view in their remote data source. Refer to "*Creating a View of a Non-OAAM Database*" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager* for information on how to create this view.

## 22.9 Loading from Non-Oracle or Non-Microsoft Server SQL Server Database

The OAAM Loader type is configured to be able to load from an Oracle or Microsoft SQL Server database. If you want to load from a different type of database, there are two steps that must be followed. You must deploy the jar file containing the JDBC driver for the database, and create properties of the following form using the Properties Editor and changing the bolded bracketed values:

```
oaam.offline.loader.databaseplatform.enum.[identifier]=[number > 10]
oaam.offline.loader.databaseplatform.enum.[identifier].name=[Human Readable Name]
oaam.offline.loader.databaseplatform.enum.[identifier].driver=[Driver Class Name]
```

> **Note:** If you add multiple database types, that [number > 10] must be unique for each one.

For example, to set up for IBM DB2, you would set the following properties:

```
oaam.offline.loader.databaseplatform.enum.db2=11
oaam.offline.loader.databaseplatform.enum.db2.name=IBM DB2
oaam.offline.loader.databaseplatform.enum.db2.driver=COM.app.db2.jdbc.app.DB2Drive
r
```

## 22.10  Changing the Checkpoints to Run

A Run Job using the OAAM Load type reads the session records from the database, applies policies for the pre-authentication and post-authentication checkpoints. Pre-authentication checkpoints are run for all sessions if the `PreAuth` property is set to true. By default it is set to true. Post-authentication checkpoints are run only for sessions where the user is successfully authenticated and the `PostAuth` property is set to true.

If you have customized checkpoints and policies in addition to or instead of our standard checkpoints and policies and you would like to change whether checkpoints run or not, you will have to create or edit the following properties using the Properties Editor:

```
profile.type.enum.[checkpoint-key].isPreAuth
or
profile.type.enum.[checkpoint-key].isPostAuth
```

Setting the `isPreAuth` or `isPostAuth` property to `true` or `false` for a given checkpoint changes which checkpoint to run. The pre-authentication checkpoints are run first and then post-authentication checkpoints are run second. The sequence of the checkpoints cannot be changed since checkpoints have a numerical order and they are run in that order.

## 22.11  Migration

Migration of custom loaders from 10*g* is not supported.

## 22.12  Use Cases

This section present common use cases for OAAM Offline and running jobs.

### 22.12.1  Use Case: Upgrading a Deployment with Multiple Scheduled Jobs

Chuck is an administrator who is expected to upgrade a 10*g* deployment with multiple scheduled jobs to 11*g* offline without any interruption in the schedule.

**Requires:** upgrade assistant

**Solution:** Chuck runs the upgrade assistant to upgrade the 10g offline to 11*g* and the scheduled jobs are migrated to the new environment.

### 22.12.2  Use Case: Configure a Solution to Run Risk Evaluations Offline

George is a security and compliance officer. He has been asked to configure a solution to run risk evaluations offline that are deemed too expensive to run in real-time. Part of the purpose of this process is to use configurable actions to provision users, devices, IPs, and other data such as locale into/out of groups to profile their behaviors.

**Requires**: Login Loader, Load/Run, Configuration Actions, and BIP

**Solution**: George exports the configured groups and imports them into the production database for use in real-time risk analysis. He uses the OAAM Loader that is already configured to pull data into the offline database and map it correctly. He also uses the out-of-the-box run task to perform the entire login chain of checkpoints on every session in the selection.

**Procedure**: In the OAAM Admin console George defines the source of the data as the OAAM production database and how much data to load (1 month) and run by

specifying a date range. He can choose to load a selection and run checkpoints on only a sub-selection of that data if he wishes. Lastly he either configures a single date/time to load and run or a reoccurring load and run or simply clicks Start to start the load and run now. (He can configure a configurable action to add users who were blocked into the "blacklisted group")

After the load and run are complete, George generates a few BI Publisher aggregate reports showing metrics for the total numbers of each action, alert, risk scores by checkpoint and total members added/removed from each profiling group.

**Outline of the general tasks and questions/issues a user faces in this flow**

- Configure data source

- Map data into useful structure - login (OOTB)

- Selection of data to load - all or a specific selection

- Run checkpoints also?

- Load now or start at a set time?

- Scheduling when the load happens or recurring

- View the results in a useful format to understand the insights found by the risk evaluations and profiling performed.

## 22.12.3 Use Case: Run Login Analysis on the Same Data Multiple Times (Reset Data)

George is a security and compliance officer. He has been asked to configure a solution to test new/edited risk evaluations offline before they are deployed to run in production.

**Requires**: OAAM Loader, Universal Risk Snapshot, and Security Policies

**Solution**: He uses the OAAM Loader that is already configured to pull data into the offline database and map it correctly. He also uses the out-of-the-box run task to perform the entire login chain of checkpoints on every session in the selection.

**Procedure**: In the OAAM Administration Console George defines the source of the data as the OAAM production database and how much data to load and run by specifying a date range. He can choose to load a selection and run checkpoints on only a sub-selection of that data if he wishes. He selects data for the last month. George then exports a snapshot from the production OAAM Admin and restores it into OAAM offline testing environment. He configures a load and run for all the data. He gives a base name for the run "Production state 08/11/2010." When the first instance of the run occurs it is automatically given a name using the base name appended with the start data/time "Production state 08/11/2010_18:01.80112010". Once the run is complete his team makes edits and additions to the security policies they had designed. George starts another run that is automatically named "Production state 08/11/2010_23:12.80112010" on all the data. This second run will ignore any data created in the first run so the results will not be skewed. Actions alerts and scores generated by the first run will not affect the results of the second run or any other run. Once the second run is complete he generates a report showing aggregate outcome values for the two runs so they can be compared side by side. George is satisfied with the results so he backs up a snapshot and restores it into the production environment.

**General tasks and questions/issues a user faces in this flow**

1. Configure data source.

2. Map data into useful structure - login (OOTB).

3. Selection of data to load - all or a specific selection?

4. Run checkpoints also?

5. Load now or start at a set time?

6. Scheduling when the load happens or reoccurring.

7. View the results in a useful format to understand the insights found by the risk evaluations and profiling performed.

### 22.12.4 Use Case: Monitor Data Rollup

Gram is an IT Administrator who must make sure the monitor data used in the dashboard is kept optimized. He must configure a consolidation of the data to automatically run three times a week from now on.

**Solution**: Gram will use the Monitor Data Rollup task that is already available to consolidate the Monitor data three times a week. He will configure the database connection properties to map to the OAAM Production database correctly.

**Procedure**: In the OAAM Administration Console (online) Gram defines the source of the data as the OAAM production database and how much data to consolidate by specifying a date range. He configures the monitor data rollup with the proper rollup unit and cutoff date. He then schedules to run the job for 3 times a week.

### 22.12.5 Use Case: Consolidation of the Dashboard Monitor Data

Gram is an IT Administrator who must make sure the monitor data used in the dashboard is kept optimized on a daily basis. He must configure a consolidation of the data to automatically run daily from now on.

**Solution**: Gram will use the Monitor Data Rollup task that is already available to consolidate the monitor data daily. He will configure the database connection properties to map to the OAAM Production database correctly.

**Procedure**: In the OAAM Administration Console (online) Gram defines the source of the data as the OAAM production database and how much data to consolidate by specifying a date range. He configures the monitor data rollup with the rollup unit as daily and cutoff time to 1. He then schedules to run the job for 3 times a week. When he views the historical dashboard, he realizes that some of the hourly granularity in the hourly trending view in the bottom part dashboard is lost which is expected.

### 22.12.6 Use Case: Load Transactional Data and Run Risk Evaluations from Multiple Sources

George is a security and compliance officer. He has been asked to configure a solution to monitor employee usage of their gas cards to identify any employees that may be abusing the resource.

**Solution**: George wants to run risk evaluations against the motor pool vehicle type data, employee details on type of vehicles used and gas card transaction records. This data comes from three different sources and is available in CSV format. George worked with his team and a contractor to develop a custom data loader that meets his requirements.

This loader maps the incoming data to the OAAM schema utilizing entities and transactions he previously defined in the OAAM Administration Console. His team also developed a custom run task to evaluate using two transaction checkpoints. They

developed the run task so administrators can select which of the two checkpoints they want to run.

**Procedure**: In the OAAM Administration Console George defines how much data to load and run by specifying a date range. He can choose to load a selection and run rules on only a sub-selection of that data if he wishes. Once George determines what data to run risk evaluations on he selects what checkpoints to run. He can select one or more to run at a time. Lastly he either configures a single date/time to load and run or a reoccurring load and run or simply clicks start to kick off the load and run now.

After the run and load and run is complete George's team runs both an aggregate and listing reports they developed. One displays total numbers of each alert per month but also trending of each alert by day of the month so they can see any spikes. The other shows the employees that triggered alerts, each with a list of the alerts they triggered and when.

**Outline of General Tasks**: Below is an outline of the general tasks and questions/issues a user faces in this flow.

- Configure data sources

- Map data into OAAM schema - Transaction (Custom)

- Selection of data to load - all or a specific selection?

- Run rules also?

- What checkpoints do I want to run?

- Load now or start at a set time?

- Scheduling when the load happens or reoccurring

- Reporting to view results in a useful form for the business users.

## 22.12.7 Use Case: Using OAAM Offline (Standard Loading)

The user flow for OAAM Offline usage is shown below.

1. Install the offline system.

2. Load data.

3. Run rules against the data.

   Checkpoint evaluation follows the same order as online.

   In post -authentication, for rules with challenge actions, the authentication status will be set to pending.

   Alerts will be generated for suspicious activities.

4. Examine dashboard and reports.

5. Discover hacking attempts.

6. Create new rules and policies to trap the attacks.

7. Run the old data through the new rules and policies.

8. Reexamine reports to see if the new rules helped.

9. Test the rules in pre-production.

10. Implement new rules and policies on Oracle Adaptive Access Manager production system.

## 22.13 Best Practices

This section outlines some best practices for administrators using OAAM Offline.

### 22.13.1 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.

### 22.13.2 Database Server with Good I/O Capability

Make sure the host that runs the database server has good I/O capability. Offline processing is I/O intensive.

### 22.13.3 Database Indexes

Make sure to obtain and apply the latest Oracle Adaptive Access Manager database patch to ensure that the proper indexes are present.

### 22.13.4 Setting Memory Buffer Size

Load/ Run pauses only after buffer is flushed. When there is need for pause/resume, keep the throttle size lower. The default is 100.

### 22.13.5 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.

### 22.13.6 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.

### 22.13.7  Availability

Failover is not instantaneous. The system uses a leasing mechanism to tell whether the Job is still alive, and fails over when the lease expires, which may take as much as 10 minutes.

### 22.13.8  OAAM Loader vs. File-based and Custom Loaders

The OAAM Loader is preferred over the file-based and custom loaders since the OAAM 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 storing data in a temporary database using standard tools and then using the temporary database to load data into the database.

### 22.13.9  Custom Loader Usage

Custom Loaders can be used for the following

- If the data cannot be mapped easily and requires complex SQL queries or some manipulations
- Requires custom Java code to map data
- Requires loading Transaction data
- Requires loading login and transaction data

For guidelines for developing a custom loader, refer to "Developing a Custom Loader" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

# Part VIII

## Scheduling Jobs

This part provides information about defining, scheduling, and running jobs for performing batch analysis.

# 23

# Scheduling and Processing Jobs in OAAM

The chapter describes how to define, schedule, and run Oracle Adaptive Access Manager batch jobs. This chapter contains the following topics:

- Access Control
- Introduction to OAAM Jobs
- Launching the Job Creation Wizard
- Creating Jobs
- Managing Jobs
- Editing Jobs
- Migration
- Use Cases

## 23.1 Access Control

Access permissions for the online scheduling system and offline environment are detailed in the following tables.

*Table 23–1    Online Job Scheduling System*

| Role | Access |
|------|--------|
| CSR and CSR Managers | No access |
| Fraud investigators and Investigation Managers | No access |
| System Administrators | Full access |
| Security Administrator | No access |

*Table 23–2    Offline Environment*

| Role | Access |
|------|--------|
| CSR and CSR Managers | No access |

*Table 23–2 (Cont.) Offline Environment*

| Role | Access |
|------|--------|
| Fraud investigators and Investigation Managers | Same access as online including security dashboard |
| System Administrators | Same access as online (Environment node) and full access to scheduler node |
| Security Administrator | Same access as online (everything except Environment Node) and full access to scheduler node |

## 23.2 Introduction to OAAM Jobs

For security administration, it is often required to run evaluations to detect high risk situations. For system administration, running a job to consolidate data is key to maintaining optimal performance of a system. Oracle Adaptive Access Manager provides the ability to configure batch jobs and schedule them.

A job is a collection of tasks that can be run by OAAM. You can perform a variety of jobs such as load data, run risk evaluation, roll up monitor data, and other jobs.

Table 23–3 provides descriptions for these jobs.

*Table 23–3 Jobs*

| Jobs | Applicable Deployment | Descriptions |
|------|----------------------|--------------|
| Load | offline | A Load Job records from a remote data source, converts the data into OAAM login sessions, and stores the login sessions in the OAAM offline datastore. |
| Run | offline | A Run Job performs risk analysis on a set of OAAM sessions. |
| Load and Run | offline | A Load and Run Job is a combination of a Load Job and a Run Job. After each record is processed by the Load Job, the result is fed directly into the Run Job. |
| Monitor Data Rollup | online and offline | A Monitor Data Rollup Job consolidates monitor data utilized in the dashboard and some risk evaluations on a regular basis. This job consolidates data to optimize the database when processed. |

### 23.2.1 Job Interface

The Jobs search page enables you to search for jobs to view details. Actions that you can perform on jobs are listed in this table.

*Table 23–4 Job Actions*

| Action | Description |
|--------|-------------|
| Search | Search for jobs. |
| Create | Create jobs. |
| Execute | Start running a job |
| View logs | View the log of a job |
| View execution queue | View the processing order of jobs |

*Table 23–4   (Cont.)  Job Actions*

| Action | Description |
| --- | --- |
| View progress of jobs | View the percentage complete and estimated time for completion |
| Pause and resume | Stop a job and start it again |
| Cancel jobs | Stop a job |

The Job Creation wizard is invoked by clicking the **New Job** icon and provides a step-by-step guide through the job definition and scheduling process. The wizard prompts you for information as you go. If you are using a standard loading process, you configure your database connection URL for the Data Loader to access the offline data in the remote database, the characteristics of the run session, a filter for the data to be loaded in the database, and schedule to run the job.

The Job Queue page displays the job currently processing and progress in terms of estimated completion time and percentage complete progress. You can cancel or pause and resume a job processing from the queue. If a job is not set to process via scheduling it will not appear in the Job Queue.

## 23.2.2  Job Queue

When a job is created and scheduled, a single instance of the job is added to the Job Queue. The Job Queue is the order of job execution. Processing order is based on scheduled start time, priority and date/time added to the queue. Jobs are displayed in the queue according to the order they will process.

For example, if Job A is configured with a High priority and set to process immediately, and then Job B is configured with a High priority and set to process immediately, an instance of A will appear in the queue above B. The jobs will process in that order.

## 23.2.3  Searching for Jobs

Using the Jobs search page, you can search for jobs and view their details.

1. From the Navigation tree, double-click **Jobs** to open the Jobs search page.

2. Specify criteria in the search filter to locate the job and click **Search**.

*Table 23–5    Search Filters*

| Filter | Definition |
| --- | --- |
| Job Type | The specific task that a job performs. |
| Job Status | Enabled or Disabled. A disabled job will not run. |
| Job Priority | Priority for the job: High, Low, Medium |
| Created Date | Date job was created.<br>By default, the Created Date is set to last 1 month. |
| Schedule Type | Once or Recurring. |
| Recurrence Interval | Hourly, Daily, Weekly, or Monthly |
| Last Start Date | The last start time of the job execution. When you set the "from" section of this field, the "to" section is automatically populated to the current time. |
| Last End Date | By default, the Last End Date is set to 24 hours after the Last Start Date. |

Clicking a job name opens the corresponding Job Details page in a new tab.

> **Note:** The standard jobs packaged with Oracle Adaptive Access Manager support a number of languages. However, the job name, Default Monitor Data Rollup Task, is displayed in English, even if you are viewing non-English content.

From the Jobs search page, you can perform the following tasks from the toolbar:

**Table 23–6    Results Table Toolbar Actions**

| Action | Description |
| --- | --- |
| Open | Open the job to see details. |
| Delete | Delete the job. |
| Enable | Enable the job. |
| Disable | Disable the job. |
| Process Now | Process the job immediately. |
| Launch the Job Creation wizard | Launch the Job Creation wizard so that you can define and schedule a job. |

## 23.3  Launching the Job Creation Wizard

Use the Job Creation wizard to create a new job. Jobs are created by the Security Administrator in Online application or by the Security Administrator or System Administrator in Offline application. The Monitor Data Rollup Job is created by the System Administrator.

To open the Job Creation wizard, perform the following steps:

1. From the Navigation tree, double-click **Jobs** to open the Jobs search page.

2. Click the **New Job** button on the upper right of the Console or the **New Job** button on the toolbar or select **New Job** from the Actions menu.

   The New Job dialog appears with the available job types to select from.

   > **Note:** All jobs listed in the table are available in OAAM Offline. Only Monitor Data Rollup is available for OAAM Online.

**Table 23–7    OAAM Job Types**

| Job Type | Definitions |
| --- | --- |
| Load | Read data to create OAAM sessions. |
| Load and Run | Create and read OAAM sessions in one step. |
| Monitor Data Rollup | Monitor data consolidation |
| Run | Perform bulk risk analysis on OAAM sessions |

3. Select the job you want to create and click **Continue**.

   The General page opens by default as the first page of the Job Creation wizard.

The following sections describe the pages of the Job Creation wizard. On these pages, required settings are identified by the asterisk (*).

### 23.3.1 Create Job: General

The General page displays general information about the job such as job type, job name, and job status. Use this page to name and describe the job. The Job Name field can take alphanumeric characters. The job is enabled by default.

---

**Note:** The job type cannot be changed.

---

### 23.3.2 Create Job: Load Details (for Load and Load and Run Jobs)

The Load Details page allows you to control which records will be processed.

You can choose between the Custom Loader and the OAAM Loader.

*Table 23–8   Custom and OAAM Loaders*

| Loaders | Description |
| --- | --- |
| Custom Loader | A Custom Loader is a user-defined loader that defines how to accomplish complex and custom scenarios. |
| | For the custom loader, you must provide the fully qualified class name for the custom loader class. |
| OAAM Loader | The OAAM Loader is the default loader that defines how the records are read from the remote data source and how they are converted into OAAM sessions. |
| | The OAAM Data Loader loads login data from a relational database. |

By default, the OAAM Loader is selected. It requires information on the data source, data mapping, and miscellaneous properties.

*Table 23–9   OAAM Loader Details*

| Panels | Description |
| --- | --- |
| Data Source | This panel contains the information about the data source and connection information. |
| Data Mapping | This panel provides information about the mapping between the OAAM offline database and the database from which the data is loaded. This is usually pre-populated for OAAM schemas. |
| Miscellaneous properties | This panel contains other information such as transaction size, memory buffer size, and write pool size and the values can be adjusted to improve performance. |

### 23.3.3 Create Job: Run Details (for Run and Load and Run Jobs)

The Run Details page lets you choose the Custom Run Type or the OAAM Run Type. The Run type defines how and under what conditions the OAAM policies are applied to the sessions.

### 23.3.4 Create Job: Data Filters

The Data Filters page allows you to choose the filter that decides which set of data to load into the offline system or process. If the job type is Load and Run, then the same data filter applies for both load and run.

The Auto Increment filter defines the set of records as all records created after the date specified in the **From Date** field. The Date Range filter defines the set of records as all records that were created between the dates specified in the **From Date** and **To Date** fields.

## 23.3.5  Create Job: Schedule

The Schedule page allows you to specify the scheduling options for the job. You provide the following information:

*Table 23–10    Schedule Page Options*

| Options | Description |
| --- | --- |
| Job Priority | The job priority determines the importance of the job and the job will be added to the job execution queue based on the priority. For additional information, refer to Section 23.3.5.1, "Job Priority." |
| Schedule Type | You can choose to run the job immediately or you can schedule the job to run in the future. For information, refer to Section 23.3.5.2, "Schedule Type." |
| Start Date and Start Time (Once) | The job runs at the Start Date and Time. |
| Recurrence Interval (Recurring) | Daily Hourly, Weekly, Monthly<br><br>The job repeats execution based on your selection. |
| Execute Every (Recurring) | Recurrence frequency of the recurrence interval. For example if the Recurrence Interval is Weekly, you could enter 2 for Execute Every. The job will execute every 2 weeks |
| Start Time (Recurring) | The recurring job starts at the time you specified on the Start Date given in the Recurrence Range.<br><br>You can pick the day of the week by selecting a begin time that is on the day of the week that you want. |
| Start Date and End Date for Recurrence Range (Recurring) | This is the date range for job execution. The job will continue execution between the Start date and End Date at intervals specified by you. For a recurring job, the Start Date is the date and time at which the job will first executes. The End Date is the date and time after which there will be no more recurrences. If left blank, the job will recur indefinitely until it is manually removed from the Job Queue. End Date is not applicable for a nonrecurring job. |
| Cancel execution if job runs longer than | The job cancels if it runs longer than a certain time. For example: 60 seconds. The job cancels execution if runtime exceeds 60 seconds. For information, refer to Section 23.3.5.3, "Cancel Time." |

### 23.3.5.1  Job Priority

Job priority indicates the importance of the job. Job priority can be set to low, medium and high. If two jobs are in conflict the higher priority job will process first. If two jobs are in conflict and they have the same priority, OAAM will randomly select one of the jobs to process first.

*Table 23–11  Job Priority Examples*

| Example | Set to Process | Priority | Result when administrator clicks Submit at exactly the same time |
|---|---|---|---|
| 1 | Job A: Immediately<br><br>Job B: Immediately | Job A: High<br><br>Job B: Medium | Instance of A will show up in the queue above Instance of B and will process in that order because Job A is higher priority |
| 2 | Exactly the same start time/date | Job A: Medium<br><br>Job B: Low | Instance of A will show up in the queue above Instance of B and will process in that order because Job A is higher priority. |
| 3 | Exactly the same start time/date | Both are Medium | Job queue logic will select either A or B randomly to process first and instances will display in the Job Queue in the randomly determined order |

### 23.3.5.2  Schedule Type

Schedule Type determines how often and when a particular job will be run. Schedule Type is either **Once** or **Recurring**.

*Table 23–12  Scheduling Types*

| Type | Definition | Fields Required | Fields that Do Not Apply |
|---|---|---|---|
| Once | Run the job once and only once at the date and time specified in the future.<br><br>If the schedule type is set to Once, the execution time (Start Date and Start Time) is set to the current date and time by default and the job processes at once ("now"). | Start Date and Start Time | Recurrence/Interval Type, Recurrence Frequency, or End Time |
| Recurring | Run the job multiple times on a schedule | All<br><br>Frequency is how often the execution recurs. | None |

Examples of scheduling types are shown in the following table.

*Table 23–13   Scheduling Type Examples*

| If I want | Values to set are | Notes |
|---|---|---|
| A group of related and dependent jobs to run every two weeks | ■ Recurrence/Interval Type: Weekly<br>■ Recurrence Frequency: 2 | |
| Job to run every two weeks on a Monday at 3:00PM, from August 30, 2010 until October 25, 2010 | ■ Schedule Type: Recurring<br>■ Begin Time: 08/30/2010 3:00 PM<br>■ End Time: 10/25/2010 3:00 PM<br>■ Interval: Weekly<br>■ Frequency: 2<br>■ Time: 3:00 PM | The user does not specify the day of week directly. For weekly recurrence, the user indirectly picks the day of week by selecting a begin time that is on the day of week that she wants. This example the job will run on Mondays because 08/30/2010 is a Monday. |

### 23.3.5.3 Cancel Time

As part of your job definition, you can specify an optional **Cancel Time**. The **Cancel Time** determines the maximum amount of time a job is allowed to run before the system automatically stops it. In this way, users can avoid the problem of having jobs run at times that may conflict with other activities. This option is not required, and if a job has no cancel time, it will run until it finishes or until a user manually stops it. If the job is currently executing, then changing the cancel time will only affect future recurrences. The currently executing job instance will use the original setting.

## 23.3.6 Create Job: Summary

The Summary page displays the choices made and information entered on the previous wizard pages.

# 23.4 Creating Jobs

Create new jobs by following the instructions in this section. Topics covered in this section are:

■ Creating Load Jobs

■ Creating Run Jobs

■ Creating Load and Run Jobs

■ Creating Monitor Data Rollup Jobs

## 23.4.1 Creating Load Jobs

A Load Job reads records from a remote data source, converts the data into OAAM login sessions, and stores the login sessions in the OAAM offline datastore.

> **Note:** If you are loading from a non-OAAM schema, you must set up a database view. For instructions, refer to "*Creating a View of a Non-OAAM Database*" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

The process for creating a Load Job is:

1. Select Job Type and provide job details. See Section 23.4.1.1, "Selecting Load Job Type and Providing Job Details."

2. Enter Load Details.

   The Loader type defines how the records are read from the remote data source and how they are converted into OAAM sessions.

   If you want to load data from a database, choose the OAAM Loader Type that is shipped with OAAM. See Section 23.4.1.3, "Providing Load Details for OAAM Data Loader."

   If you want to perform any other type of task, choose a Custom Loader Type. See Section 23.4.1.2, "Providing Load Details for Custom Loader."

   If using the OAAM Loader Type, the following steps are needed:

3. Set up the data filter.

   The data filter defines a criteria to define the set of records in the database to be loaded or run.

   If you want to define the set of records as all records created after a given date, choose **Auto Increment** as the data filter type. See Section 23.4.1.4, "Specifying to Load All Data Created After a Given Date."

   If you want to define the set of records as all records that were created between a From Date and a To Date, choose **Date Range**. See Section 23.4.1.5, "Specifying to Load Data Created within a Date Range."

4. Set up the scheduling.

   If you want to schedule a Load Job that runs once, choose **Once** as the schedule type. See Section 23.4.1.6, "Scheduling a Load Job that Runs Once."

   If you want to schedule a Load Job that runs on a regular basis, choose **Recurring** as the schedule type. See Section 23.4.1.7, "Scheduling a Load Job that Runs on a Regular Basis (Recurring)."

5. Confirm details. See Section 23.4.1.8, "Checking the Summary Details of Load Job."

### 23.4.1.1 Selecting Load Job Type and Providing Job Details

To create a Load Job:

1. From the Jobs search page, click the **New Job** button.

   The **Choose Job Type** dialog appears with the available job types to select from.

2. Select **Load** and click the **Continue** button

   The Create Job page opens to the General page where you can specify the name and description for the Load Job.

   By default the status is **Enabled** and the **Job Type** field displays **Load**.

   The **Job Type** field is not editable.

3. Decide on a name for the job you are defining and enter it in the **Job Name** field.

   The Job Name can only contain alphanumeric characters.

4. Enter a description for the Load Job.

   The **Next** button is enabled after the job name and description have been entered.

5. Click the **Next** button to create the Load Job.

The job is created and you are directed to the **Load Details** page.

### 23.4.1.2 Providing Load Details for Custom Loader

A Custom Loader is a user-defined loader that defines how to accomplish complex and custom scenarios. After creating the job, you are directed to the Load Details page where you can start defining the job.

If you want to use a custom loader to load the data source, follow these steps:

1.  In the Load Details page, select **Custom Loader**.

    This is the custom loader you developed to accomplish complex and custom scenarios specific to your deployment. You will have written a custom class to define this loader.

2.  To select a custom loader, click the **Update Class Path...** button.

    A dialog appears where you must enter the exact path of a Java class that implements the custom loader specification.

3.  Enter the exact path of a Java class that implements the custom loader specification and press **OK**.

    If the system cannot find the class, or if the class is not a properly defined custom loader, an error occurs.

### 23.4.1.3 Providing Load Details for OAAM Data Loader

The loader type defines how the records are read from the remote data source and how they are converted into OAAM sessions. After creating the job, you are directed to the Load Details page where you can start defining the job.

The OAAM Data Loader loads login data from a relational database. If you want the OAAM Loader as the data loader type for your data source, follow these steps.

1.  In the Load Details page, ensure that the **OAAM Loader** type is selected.

2.  Under Data Source Details, enter the database connection parameters for the source database.

    The **Database Connection** and **Data Mapping** sections of Data Source Details only exist for the OAAM Loader.

    The database connection parameters define how to connect to the remote database.

*Table 23–14   Database Connection Parameters*

| Parameter | Description |
| --- | --- |
| Database Platform | The type of database from which you will be loading. |
| JDBC URL | The connection string for the database. |
| Database User Schema | The user name for the database. |
| Database Password | The password for the database. |

3.  Enter values for the miscellaneous properties.

    This panel contains information that can be adjusted to improve performance such as transaction size, memory buffer size, and write pool size.

*Table 23–15    Characteristics of the Load Job*

| Property | Description |
| --- | --- |
| Write Pool Size | Defines the number of threads dedicated to processing the incoming records. The optimal value will depend on the users' systems, so users may have to experiment to find the value that gives them the best performance on their system. |
| Memory Buffer Size | Defines the size of the buffer that holds yet-to-be processed records in memory. When pausing or suspending a job that is meant to restart, all records in this buffer must be processed before the job can stop. The higher this value is, the longer the shutdown procedure will take. |
| Transaction Size | Defines how records are processed as a batch, and also controls the logging frequency. |

4. Click the **Next** button.

   After providing the database connection details and adjusting various properties in the Load Details page, you are ready to apply data filters for the Load Job.

### 23.4.1.4  Specifying to Load All Data Created After a Given Date

After entering the required database connection parameters and miscellaneous properties in the Load Details page, you are directed to the Data Filters page where you can specify which set of data to load. Data filters determine which set of records should be loaded into the offline system.

If you want to define the set of records as all records created after a given, follow these steps.

1. Select **Auto Increment** as the filter type.

2. Enter a **From Date**.

3. Click the **Next** button.

   You are directed to the Schedule page where you can specify to run the job once or on a recurring basis.

   A recurring Load Job with an Auto Increment filter will suspend itself after it processes all records that meet its criteria, and the next recurrence will process any new records that have been added in the mean time. If you decide to apply the **Auto Increment** filter, then the best practice is to use a **Recurring** schedule for the Load Job.

### 23.4.1.5  Specifying to Load Data Created within a Date Range

After entering the required database connection parameters and miscellaneous properties in the Load Details page, you are directed to the Data Filters page where you can specify the data filter to use to define the set of records to be loaded. A Date Range filter defines the set of records as all records that were created between a **From Date** and a **To Date**.

If you want data within a date range to be loaded from the data source, follow these steps.

1. Select **Date Range** as the filter type.

2. Enter a **From Date** and **To Date**.

   Only data that falls within that specific date range is loaded. You will need to enter the **From** and **To Date** for data collection. All data processed within these dates are loaded into the offline system.

**3.** Click the **Next** button.

You are directed to the Schedule page where you can specify to run the job once or on a recurring basis.

### 23.4.1.6 Scheduling a Load Job that Runs Once

After specifying the data filter, you are directed to the Schedule page where you can define the priority and schedule type for your job.

If you want the job to run immediately, follow these steps:

**1.** In the Schedule page, select a job priority: **High**, **Medium** or **Low**.

Job priority determines the importance of the job.

**2.** Select **Once** as the **Schedule Type**.

The job runs at the start date and start time specified by you or the job can be run immediately. This job is run only once and there is no recurrence. If the schedule type is set to **Once**, the execution time (Start Date and Start Time) is set to the current date and time and the job at once ("now").

**3.** Enter the **Start Date** and **Start Time** under Schedule Details.

**4.** Choose the **Cancel execution if runs longer than** option.

The job cancels if it runs longer than a certain time.

For example: 60 seconds. The job cancels execution if runtime exceeds 60 seconds.

**5.** Click **Next**.

### 23.4.1.7 Scheduling a Load Job that Runs on a Regular Basis (Recurring)

After specifying the data filter, you are directed to the Schedule page where you can define the priority and schedule type for your job.

If you want the job to run on a regular basis, follow these steps:

**1.** In the Schedule page, select the job priority.

Job priority determines the importance of the job.

**2.** Select **Recurring** as the schedule type.

Although the schedule type can be set or modified later, you must specify a schedule type now; otherwise, you will not be able to execute the job.

The job should run repeatedly based on the recurring interval specified.

If a job is recurring, then only one job instance for a particular job may execute at once. If the previous recurrence is still running, paused, or waiting in the Job Queue to execute, then this job instance is skipped. The job instance is moved to the job log with a status of **Skipped**, and the next recurrence, if any, is placed into the Job Queue.

**3.** Set the schedule details to the desired values.

*Table 23–16    Schedule Details*

| Parameters | Description |
| --- | --- |
| Recurrence Interval | Daily Hourly, Weekly, Monthly,<br><br>The job repeats execution based on your selection. |
| Execute Every | Recurrence frequency of the recurrence interval. For example if the Recurrence Interval is Weekly, you could enter 2 for Execute Every. The job will execute every 2 weeks |
| Start Time | The recurring job starts at the time you specified on the Start Date given in the Recurrence Range. |
| Start Date and End Date for Recurrence Range | This is the date range for job execution. The job will continue execution between the Start date and End Date at intervals specified by you. For a recurring job, the Start Date is the date and time at which the job will first executes. The End Date is the date and time after which there will be no more recurrences. If left blank, the job will recur indefinitely until it is manually removed from the Job Queue. End Date is not applicable for a nonrecurring job. |
| Cancel execution if job runs longer than | The job cancels if it runs longer than a certain time.<br><br>For example: 60 seconds. The job cancels execution if runtime exceeds 60 seconds. |

**4.** Click **Next** if you want to see the Summary page or click **Finish** to process the job.

### 23.4.1.8  Checking the Summary Details of Load Job

If you clicked **Next** on the Schedule page, you are directed to the Summary page. This page displays the choices made and information entered on the previous wizard pages.

If you are not satisfied with the choices and entries shown on the Summary page, use the **Back** button to return to the wizard pages and make changes.

If you are satisfied with the choices and entries shown on the Summary page, create the job by clicking the **Finish** button. A success confirmation message is presented and the Job Edit page is launched. The Job Edit page allows you to modify and reschedule a job.

## 23.4.2  Creating Run Jobs

A Run Job performs risk analysis on a set of OAAM sessions. A Run Job using the OAAM Load type reads the session records from the database, applies policies for pre-authentication and post-authentication checkpoints where the user is successfully authenticated.

> **Note:**   You can change which checkpoint is pre-authentication or post-authentication by creating or editing the following properties using the Properties Editor:
>
> `profile.type.enum.[checkpoint-key].isPreAuth`
>
> `profile.type.enum.[checkpoint-key].isPostAuth`
>
> For information on checkpoint creation, refer to Section 15.1, "Creating a New Checkpoint."
>
> A Custom Run Job may perform other tasks or resolve the checkpoints to be run in a different fashion.

The process for creating a Run Job is:

1. Select Job Type and provide job details. See Section 23.4.2.1, "Selecting Run Job Type and Providing Job Details."

2. Enter Run Details. See Section 23.4.2.2, "Choosing Default or Custom Run as Run Type."

   The Run Type defines how and under what conditions the OAAM policies are applied to the sessions.

   If using the OAAM Run Type, the following steps are needed:

3. Set up the data filter.

   The data filter defines a criteria to define the set of records in the database to be loaded or run.

   If you want to define the set of records as all records created after a given date, choose **Auto Increment** as the data filter type. See Section 23.4.2.3.2, "Specifying to Run Analysis on All Data Created After a Given Date."

   If you want to define the set of records as all records that were created between given dates, choose **Date Range**. See Section 23.4.2.3.1, "Specifying to Run Analysis on Data Created Within a Date Range."

4. Set up the scheduling.

   If you want to schedule analysis to run once, choose **Once** as the schedule type. See Section 23.4.2.4.1, "Scheduling Analysis to Run Once."

   If you want to schedule analysis to run on a regular basis, choose **Recurring** as the schedule type. See Section 23.4.2.4.2, "Scheduling Analysis to Run on a Regular Basis (Recurring)."

5. Confirm details. See Section 23.4.2.5, "Checking the Summary Details of the Run Job."

### 23.4.2.1  Selecting Run Job Type and Providing Job Details

To create a Run Job, follow these steps:

1. From the Jobs search page, click the **New Job** button.

   The **Choose Job Type** dialog appears with the available job types to select from.

2. Select **Run** and click the **Continue** button.

   The Create Job page is opened by default to the General page where you can specify the name and description for the Run Job.

3. Enter a name and description for the Run Job.

   The **Next** button is enabled only after the job name and description are entered.

4. Click the **Next** button.

   The Run Job is created and you are directed to the Run Details page.

### 23.4.2.2  Choosing Default or Custom Run as Run Type

After creating the job, you are directed to the Run Details page where you can select the Run type. The Run type defines how and under what conditions the OAAM policies are applied to the sessions.

1. In the Run details page, select the Run Type from the following two options:

*Table 23–17    Run Type*

| Run Type | Description |
| --- | --- |
| Default | By default the OAAM Run type is selected. The Pre-Authentication and Post-Authentication checkpoints which are enabled by default are run. If you select the default run type, you will need to specify the Transaction Size and Memory Buffer Size. |
| Custom Run | To select a Custom Run type, click the **Update Class Path...** button, then enter the fully qualified class name for the custom run class. If it is valid, you will be able to proceed to next page; otherwise, an error message is displayed. The custom run class path is usually different from the Custom Load Class path. |

2. Click the **Next** button.

   You are directed to the Data Filters page.

### 23.4.2.3 Specifying Which Set of Records to Analyze

After selecting the Run type, you are directed to the Data Filters page where you can:

- Specify how much data to load and run by specifying a date range, or

- Choose to load a selection and run checkpoints on only a sub-selection of that data

**23.4.2.3.1  Specifying to Run Analysis on Data Created Within a Date Range**   If you want to define the set of records as all records that were created between given dates, follow these steps:

1. Select **Date Range** as the filter type.

2. Enter the **From** and **To Date** for data processing.

   All data loaded within these dates will be processed.

3. Click **Next**.

   You are directed to the Schedule page.

**23.4.2.3.2  Specifying to Run Analysis on All Data Created After a Given Date**   If you want to define the set of records as all records created after a given, follow these steps.

1. Select **Auto Increment** as the filter type.

2. Enter **From Date**.

   This is the date from when data should be run.

   All data from the given date will be processed with the current policies and rules.

3. Click **Next**.

   You are directed to the Schedule page.

### 23.4.2.4 Scheduling Analysis to Run

After specifying the data filter, you are directed to the Schedule page where you can define the priority and schedule type for your job.

You can choose to:

- Configure a single date/time to load and run

- Configure a recurring load and run

- Click Start to start the load and run now

**23.4.2.4.1 Scheduling Analysis to Run Once** To configure a single date/time to load and run:

1. In the Schedule page, select a job priority.

   Job priority determines the importance of the job.

2. Select **Once** as the **Schedule Type**.

   The job runs at the start date and start time specified by you or the job can be run immediately. This job is run only once and there is no recurrence. If the Schedule Type is set to **Once**, the execution time (Start Date and Start Time) is set to the current date and time and the job at once ("now").

3. Set the schedule details to the desired values.

*Table 23–18    Schedule Details for a Run Job that Executes Once*

| Property | Description |
| --- | --- |
| Start Date and Start Time | The job will run at the Start Date and Time. |
| Cancel Execution if job runs longer than | The maximum amount of time a job is allowed to run before the system automatically stops it. This option is not required, and if a job has no cancel time, it will run until it finishes or until a user manually stops it. |

4. Click **Next**.

**23.4.2.4.2 Scheduling Analysis to Run on a Regular Basis (Recurring)** To configure a recurring load and run:

1. At the Schedule page, select the job priority.

2. Select the **Schedule Type** as **Recurring**.

   The job should run repeatedly based on the recurring interval specified. If a job is recurring, then only one job instance for a particular job may execute at once. If the previous recurrence is still running, paused, or waiting in the Job Queue to execute, then this job instance is skipped. The job instance is moved to the job log with a status of **Skipped**, and the next recurrence, if any, is placed into the Job Queue.

3. Set the schedule details to the desired values.

   The Run Job will execute as per the Schedule Details.

*Table 23–19    Schedule Details for Recurring Run Job*

| Properties | Description |
| --- | --- |
| Recurrence Interval | Hourly, Daily, Weekly or Monthly |
| Execute Every | Frequency in the recurrence pattern |
| Start Time | The recurring job starts at the time you specified on the Start Date given in the Recurrence Range. |
| Start Date and End Date | This is the date range for job execution. The job will continue execution between the Start date and End Date at intervals specified by you. For a recurring job, the Start Date is the date and time at which the job will first executes. The End Date is the date and time after which there will be no more recurrences. If left blank, the job will recur indefinitely until it is manually removed from the Job Queue. End Date is not applicable for a nonrecurring job. |
| Cancels execution if runtime exceeds | The maximum amount of time a job is allowed to run before the system automatically stops it. This option is not required, and if a job has no cancel time, it will run until it finishes or until a user manually stops it. |

**4.** Click **Next** to proceed to the summary page or **Finish** to process the job.

### 23.4.2.5 Checking the Summary Details of the Run Job

If you clicked **Next** on the Schedule page, you are directed to the Summary page.

This page displays the choices made and information entered on the previous wizard pages. If you are not satisfied with the choices and entries shown on the Summary page, use the **Back** button to return to the wizard pages and make changes. If you are satisfied with the choices and entries shown on the Summary page, create the job by clicking the **Finish** button. A success confirmation message is presented and the Job Edit page is launched. The Job Edit page allows you to modify and reschedule a job.

#### Data Clean Up

When a Run begins executing, it performs a clean up for the records in the job's data filter. This clean up involves deleting rule logs, alerts, and actions and resetting risk scores and authentication statuses. This ensures that this data created from a run will not affect other runs on the same data. Pattern and group updates will not be reset between runs so these features are not intended for use cases where the same data is run multiple times.

For example, if you create a Run Job named "R&D Run" and you process it three times, the results (actions, alerts and score) from "R&D Run_090820100429" will not effect "R&D Run_090820100715" and "R&D Run_090920100807" will ignore outcomes of the previous two.

## 23.4.3 Creating Load and Run Jobs

A Load and Run Job is a combination of a Load Job and a Run Job. After each record is processed by the Load Job, the result is fed directly into the Run Job. In a Load and Run Job, patterns will be processed for successful logins after the post-authentication rules are processed.

> **Note:** If you are loading from a non-OAAM schema, you must set up a database view. For instructions, refer to "*Creating a View of a Non-OAAM Database*" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

### 23.4.3.1 Selecting Load and Run Job Type and Providing Details

**1.** From the Jobs search page, click the **Create Job** button.

The **Choose Job Type** dialog appears with the available job types to select from.

**2.** Select Load and Run and click the **Continue** button.

The Create Job page is opened by default to the General page where you have to specify the name and description for the Load and Run Job.

By default the **Status** should be **Enabled**.

**3.** Select **Load and Run** as the job type.

**4.** Enter a name and description for the Load and Run Job and select the status.

The job type, name and description for the Load and Run Job and the status should be displayed in the General page. By default the status should be **Enabled**.

**5.** Click the **Next** button.

The Load and Run Job is created and you are directed to the Load Details page.

### 23.4.3.2 Selecting Loader Type for Load and Run Job

After creating the job, you are directed to the Load Details page where you can start defining the job.

1.  In the Load Details page, select the **Loader** type from the following two options: **OAAM** and **Custom Loader**.

    By default the **OAAM** Loader type is selected. You can select the custom loader if you choose to write a custom class.

2.  Under Data Source Details, enter the database connection parameters for the source database. The following parameters have to be entered:

*Table 23–20    Database Connection Parameters*

| Parameter | Description |
| --- | --- |
| Database Platform | The type of database from which you will be loading. |
| JDBC URL | The connection string for the database. |
| Database User Schema | The user name for the database. |
| Database Password | The password for the database. |

3.  Verify miscellaneous properties.

    This panel contains information that can be modified to improve performance such as transaction size, memory buffer size, and so on.

4.  Click the **Next** button.

    You are directed to the Run Details page.

### 23.4.3.3 Specifying Data Filters for Load and Run Job

After entering the required database connection parameters and miscellaneous properties in the Load Details page, you are directed to the Data Filters page where you can specify the data filter to be used for the data to be loaded.

1.  Select **Auto Increment** or **Date Range** as the filter type. If **Auto Increment** is selected, enter date from when data should be loaded and run.

    The data filter selected is applied for both the Load and Run Job. All data from the given date is loaded. All data from the given date is processed with the current policies and rules.

2.  If **Date Range** Filter type is selected, enter the **From** and **To Date** for data processing.

    All data loaded within these dates will be processed.

### 23.4.3.4 Scheduling a Load and Run Job that Runs Once

After specifying the data filter, you are directed to the Schedule page where you can define the priority and schedule type for your job.

1.  In the Schedule page, select a job priority.

    Job priority determines the importance of the job.

2.  Select **Once** as the **Schedule Type**.

The job runs at the start date and start time specified by you or the job can be run immediately. This job is run only once and there is no recurrence. If the schedule type is set to **Once**, the execution time (Start Date and Start Time) is set to the current date and time and the job at once ("now").

3. Set the schedule details to the desired values.

*Table 23–21    Schedule Details for a Run Job that Executes Once*

| Property | Description |
| --- | --- |
| Start Date and Start Time | The job will run at the Start Date and Time. |
| Cancel Execution if job runs longer than | The maximum amount of time a job is allowed to run before the system automatically stops it. This option is not required, and if a job has no cancel time, it will run until it finishes or until a user manually stops it. |

4. Click **Next**.

### 23.4.3.5  Scheduling a Load and Run Job that Runs on a Regular Basis (Recurring)

After specifying the data filter, you are directed to the Schedule page where you can define the priority and schedule type for your job.

1. In the Schedule page, select the job priority and select schedule type as **Recurring**.

   The job should run repeatedly based on the recurring interval specified.

   If a job is recurring, then only one job instance for a particular job may execute at once. If the previous recurrence is still running, paused, or waiting in the Job Queue to execute, then this job instance is skipped. The job instance is moved to the job log with a status of **Skipped**, and the next recurrence, if any, is placed into the Job Queue.

2. Set the schedule details to the desired values.

   The Load and Run Job executes as per the Schedule Details. The Load Job runs first and then the Run Job as per the schedule details.

*Table 23–22    Schedule Details*

| Parameters | Description |
| --- | --- |
| Recurrence Interval | Daily Hourly, Weekly, Monthly |
| | The job should repeat execution based on your selection. |
| Execute Every | Recurrence frequency of the recurrence interval. For example if the Recurrence Interval is Weekly, you could enter 2 for Execute Every. The job will execute every 2 weeks |
| Start Time | The recurring job starts at the time you specified on the Start Date given in the Recurrence Range. |
| Recurrence Range: Start Date and End Date | This is the date range for job execution. The job will continue execution between the Start date and End Date at intervals specified by you. For a recurring job, the Start Date is the date and time at which the job will first executes. The End Date is the date and time after which there will be no more recurrences. If left blank, the job will recur indefinitely until it is manually removed from the Job Queue. End Date is not applicable for a nonrecurring job. |
| Cancel execution if job runs longer than | The job cancels if it runs longer than a certain time. |
| | For example: 60 seconds. The job cancels execution if runtime exceeds 60 seconds. |

3. Click **Next**.

You are directed to a summary details page.

### 23.4.3.6 Checking the Summary Details of the Load and Run Job

If you clicked **Next** on the Schedule page, you are directed to the Summary page.

This page displays the choices made and information entered on the previous wizard pages. If you are not satisfied with the choices and entries shown on the Summary page, use the **Back** button to return to the wizard pages and make changes.

If you are satisfied with the choices and entries shown on the Summary page, create the job by clicking the **Finish** button. A success confirmation message is presented and the Job Edit page is launched. The Job Edit page allows you to modify and reschedule a job.

## 23.4.4 Creating Monitor Data Rollup Jobs

This section shows how Monitor Data Rollup Jobs can be created. The topics in this section are the following:

- About Monitor Data Rollup Jobs

- Selecting Monitor Data Rollup Type and Providing Details

- Specifying Rollup Unit and Cutoff Time

- Scheduling a Monitor Data Rollup Job that Runs Once

- Scheduling a Monitor Data Rollup that Runs on a Regular Basis (Recurring)

- Checking the Summary Details of the Monitor Data Rollup

### 23.4.4.1 About Monitor Data Rollup Jobs

The Monitor Data Rollup Job reclaims space in the database by merging redundant records in the V_MONITOR_DATA table. If Monitor Data records are of the same type, with the same data value and fingerprint, and fall within the same period on a trending graph for a particular scale, then those records are considered to be redundant for that scale.

A Monitor Data Rollup Job with a daily scale, for example, will merge all of the redundant records from each day into single records for each day.

Monitor Data records may be redundant on one scale, but not redundant on a more granular scale. For example, if there are two Monitor Data records of the same type and with the same data value and fingerprint, one created on a Monday and one created two days later, then those two records would be redundant on a weekly scale, but would not be redundant on a daily scale.

When Monitor Data records are merged, each set of redundant Monitor Data records is taken and a new record is created using the earliest begin date, the latest end date, the sum of the counts and running times, the smallest minimum running time, and the largest maximum running time of each set. Then the entire set of redundant Monitor Data records is deleted and the new merged Monitor Data record is inserted to take their place. Depending on the scale at which to roll up, there will be at most one Monitor Data record for each time period for each unique combination of Monitor Type, data value, and fingerprint.

### 23.4.4.2 Selecting Monitor Data Rollup Type and Providing Details

To create a Monitor Data Rollup Job, follow these steps:

1. From the Navigation tree, double-click **Jobs** to open the Jobs search page.

2. From the Jobs search page, click the **Create Job** button.

   The **Choose Job Type** dialog appears with the available job types to select from.

3. Select **Monitor Data Rollup** and click the **Continue** button.

   The Create Job page is opened by default to the General page.

4. Select **Monitor Data Rollup** as the job type.

5. Enter a name and description for the Monitor Data Rollup Job.

6. Select the status.

   By default the status should be **Enabled**.

7. Click the **Next** button.

   The Monitor Data Rollup Job is created and you are directed to the Rollup Details page.

### 23.4.4.3 Specifying Rollup Unit and Cutoff Time

After creating the Monitor Data Rollup Job, you are directed to the Rollup Details page where you can specify Rollup options for this job. All records within the specified unit size will be rolled up (compacted) into a single record.

1. In the Rollup Details page, select the rollup unit.

   The rollup unit defines the scale at which the Monitor Data records will be rolled up.

   Choices are **Hourly**, **Days**, **Weekly**, and **Monthly**.

2. Select the Cutoff Time.

   This value determines which records should be compacted. For example, if the 6 Months is specified for the Cutoff Time, all records older than 6 months will be compacted to a single record. The Cutoff Time property tells the job which records to leave alone and not roll up.

   It is recommended that the Cutoff Time remains at the default value because if the Cutoff Time value is below the default value, the dashboard graphs may not be accurate.

*Table 23–23    Default Value for Cutoff Time*

| Rollup | Cutoff Time |
| --- | --- |
| Hourly | 1 hour |
| Days | 2 days |
| Weekly | 13 weeks |
| Monthly | 6 months |

3. Click **Next**.

### 23.4.4.4 Scheduling a Monitor Data Rollup Job that Runs Once

After specifying the Rollup options for the job, you are directed to the Schedule page where you can define the priority and schedule type for your job.

To specify for the Monitor Data Rollup Job to occur once, follow these steps:

1. In the Schedule page, select a job priority.

Job priority determines the importance of the job.

**2.** Select **Once** as the schedule type.

The job runs at the start date and start time specified by you or the job can be run immediately. This job is run only once and there is no recurrence. If the schedule type is set to **Once**, the execution time (Start Date and Start Time) is set to the current date and time and the job processes at once ("now") by default.

**3.** Set the schedule details to the desired values.

*Table 23–24   Schedule Details for a Run Job that Executes Once*

| Property | Description |
|---|---|
| Start Date and Start Time | The job will run at the Start Date and Time. |
| Cancel Execution if job runs longer than | The maximum amount of time a job is allowed to run before the system automatically stops it. This option is not required, and if a job has no cancel time, it will run until it finishes or until a user manually stops it. |

**4.** Click **Next**.

### 23.4.4.5 Scheduling a Monitor Data Rollup that Runs on a Regular Basis (Recurring)

After specifying the Rollup options for the job, you are directed to the Schedule page where you can define the priority and schedule type for your job.

To specify for the Monitor Data Rollup Job to be recurring, follow these steps:

**1.** In the Schedule page, select the job priority.

The job priority for the rollup job is set which determines the order of execution when two jobs have same schedule date and time.

**2.** Select **Recurring** as the schedule type.

The job should run repeatedly based on the recurring interval specified. If a job is recurring, then only one job instance for a particular job may execute at once. If the previous recurrence is still running, paused, or waiting in the Job Queue to execute, then this job instance is skipped. The job instance is moved to the job log with a status of **Skipped**, and the next recurrence, if any, is placed into the Job Queue.

**3.** Set the schedule details to the desired values.

*Table 23–25   Schedule Details*

| Parameters | Description |
|---|---|
| Recurrence Interval | Daily Hourly, Weekly, Monthly, <br><br>The job should repeat execution based on your selection. |
| Execute Every | Recurrence frequency of the recurrence interval. For example if the Recurrence Interval is Weekly, you could enter 2 for Execute Every. The job will execute every 2 weeks |

*Table 23–25   (Cont.)  Schedule Details*

| Parameters | Description |
|---|---|
| Start Time | The recurring job starts at the time you specified on the Start Date given in the Recurrence Range. |
| Recurrence Range: Start Date and End Date | This is the date range for job execution. The job will continue execution between the Start date and End Date at intervals specified by you. For a recurring job, the Start Date is the date and time at which the job will first executes. The End Date is the date and time after which there will be no more recurrences. If left blank, the job will recur indefinitely until it is manually removed from the Job Queue. End Date is not applicable for a nonrecurring job. |
| Cancel execution if job runs longer than | The job cancels if it runs longer than a certain time.<br><br>For example: 60 seconds. The job cancels execution if runtime exceeds 60 seconds. |

The Monitor Data Rollup Job should execute as per the Schedule Details.

4.  Click **Next**.

You are directed to the Monitor Data Rollup Job Summary Details page

### 23.4.4.6  Checking the Summary Details of the Monitor Data Rollup

If you clicked **Next** on the Schedule page, you are directed to the Summary page. This page displays the choices made and information entered on the previous wizard pages.

If you are not satisfied with the choices and entries shown on the Summary page, use the **Back** button to return to the wizard pages and make changes.

If you are satisfied with the choices and entries shown on the Summary page, create the job by clicking the **Finish** button. A success confirmation message is presented and the Job Edit page is launched.

## 23.5  Managing Jobs

This section shows how jobs can be managed in OAAM. The topics in this section are the following:

- About Running Jobs
- Notes About Rescheduling Jobs
- Processing a Job Immediately
- Pausing a Job
- Resuming a Paused Job
- Canceling a Job
- Enabling Jobs
- Disabling Jobs
- Deleting Jobs
- Viewing Job Details
- Viewing Instances of a Job
- Viewing the Job Log
- Viewing and Sorting the Job Queue

- [Editing Jobs](#)

- [Editing the Monitor Data Rollup](#)

## 23.5.1 About Running Jobs

When the scheduled start time for a job instance arrives, the system checks to see if it is allowed to execute it. If a job is recurring, then only one job instance for a particular job may execute at once, so if the previous recurrence is still running, paused, or sitting in the Job Queue waiting to execute, then this job instance will be skipped. The job instance will be moved to the job log with a status of Skipped, and the next recurrence, if any, will be placed into the Job Queue.

If the server stops while a job instance is executing, that job instance will automatically restart at the point where it stopped when the server starts up. In a clustered environment, if the server where a job instance is running fails, another server in the cluster will automatically restart it.

If the job was scheduled with a **Cancel Time**, and the server starts some time later, the time during which the server was down will not count against the elapsed time for purposes of determining when the job should auto-suspend. For example, if a job is scheduled to start at 12:00 am and cancel after two hours, but the server stops at 1:30 am and is not restarted until 7:00 am, then the job will restart where it left off at 7:00 with 30 minutes remaining, and will auto cancel at 7:30.

### 23.5.1.1 Bulk Risk Analytics Job Execution

The Load, Run, and Load and Run Job types are all mutually exclusive with each other. No Load, Run, or Load and Run Job may execute at the same time as another Job of either Job Type.

### 23.5.1.2 Run Data Reset

Actions, alerts and rule log data will be deleted if the same selection of data has another run processed on it. This ensures that this data created from a run will not affect other runs on the same data. Pattern and group updates will not be reset between runs so these features are not intended for use cases where the same data is run multiple times.

For example, if an administration console user creates a Run Job named "R&D Run" and he processes it three times, the results (actions, alerts and score) from "R&D Run_090820100429" will not effect "R&D Run_090820100715" and "R&D Run_090920100807" will ignore outcomes of the previous two.

### 23.5.1.3 Group Populations

If a configurable action adds or removes members to or from a group as a result of a run these changes will be available for use by subsequent runs.

For information on groups, refer to Chapter 12, "Managing Groups."

### 23.5.1.4 Pattern Buckets and Memberships

Pattern buckets created and membership count updates that occur as a result of a run are available for use by subsequent runs.

For information on pattern buckets and membership, refer to Section 17.1.2, "Patterns."

### 23.5.1.5 Actions, Alerts, Scores

Rule outcomes from a run will be deleted before subsequent runs on the same data.

For information on actions, alerts, and scores as outcomes, refer to Section 10.1, "Introduction to Policies, Rules, and Conditions."

### 23.5.2 Notes About Rescheduling Jobs

OAAM does not reschedule a job unless the start time is changed. When changing the recurrence pattern for a job (recurrence interval and/or recurrence frequency), the best practice is to also change the start date and time to be explicit about when you want the next recurrence to occur. Otherwise, the next scheduled recurrence, if any, will proceed as scheduled, and the next recurrence after that will be calculated from that point. If the job does not have any future recurrences scheduled, then modifying the recurrence pattern without changing the start time will have no effect -- after the change is saved, the job will still not have any future recurrences scheduled.

### 23.5.3 Processing a Job Immediately

To process a job immediately:

1. Search for the jobs that you want to enable by performing the procedure described in Section 23.2.3, "Searching for Jobs."

2. Select the job from the Search Results table and click **Process Now**.

   Alternatively, you can select **Process Now** from the Actions menu.

   If there are no other jobs that are currently running, the job is placed as a job instance in the queue. The job status is "Running" and the Start time is set to the current time.

   If another job is currently running that prevents the selected job from executing, a message informs you that the job could not be started and the queue will be unchanged.

### 23.5.4 Pausing a Job

To pause a job, if it is running, or prevent execution of a job, but leave it in the queue, follow these steps:

1. From the Job Queue page, select the job.

2. Press the **Pause** icon on the Results toolbar.

   The job instance is suspended. The next job in the queue is run. Pausing the job does not affect the order of the job instances in the execution queue.

   If a recurring job instance that has not yet started is paused, the job instance is suspended and remains paused in the queue until it is resumed or canceled.

   If a recurring job instance is paused and then resumed when another job is scheduled to run, the job that is resumed has higher priority.

### 23.5.5 Resuming a Paused Job

To resume a paused job, follow these steps:

1. From the Job Queue page, select the paused job.

   The Process button is enabled when a job instance is paused.

2. Press the **Process** icon on the Results toolbar.

The job instance resumes processing from where it was paused if no other job is currently running. The process start time shows the original process Start Time and not the Start Time when the job instance was resumed.

If a job is resumed when another job is scheduled to run, the job that is scheduled is skipped.

If another job is already running, resuming the paused job places the job in the Job Queue and it will be executed after the current job completes running.

### 23.5.6 Canceling a Job

To stop the job instance if it is running and remove the job instance from the Job Queue, perform the following steps:

1. From the Job Queue page, select the job.

2. Press the **Cancel** icon on the Results toolbar.

   The job instances that were selected are suspended and removed from the Job Queue.

   If the job is recurring, the next instance will be added to the Job Queue.

### 23.5.7 Enabling Jobs

In addition to creating and modifying jobs, you can enable jobs that are currently disabled. If the **Enable** button is enabled, it means that jobs are currently disabled and you can enable them by clicking **Enable**. If there are no disabled jobs listed in the search results table, then the **Enable** button is disabled.

To enable jobs:

1. Search for the jobs that you want to enable by performing the procedure described in Section 23.2.3, "Searching for Jobs."

2. In the search results table, select the jobs and click **Enable**.

   Alternatively, you can select **Enable** from the Actions menu.

   A message indicating that the jobs have been successfully enabled is displayed.

3. Click **OK** to close the dialog.

### 23.5.8 Disabling Jobs

You can disable jobs that are currently enabled. If the Disable button is enabled, it means that jobs are currently enabled and you can disable them by clicking Disable. If all the jobs in the search results table are disabled then the **Disable** button will not be enabled.

Only jobs that are processed can be disabled. The jobs that are running or scheduled to run in the future cannot be disabled.

To disable jobs:

1. Search for the jobs that you want to disable by performing the procedure described in Section 23.2.3, "Searching for Jobs."

2. In the search results table, select the jobs and click **Disable**.

   Alternatively, you can select **Disable** from the Actions menu.

   A message indicating that the jobs have been successfully disabled is displayed.

3. Click **OK** to close the dialog.

## 23.5.9 Deleting Jobs

To delete jobs, follow these steps:

1. Search for the jobs that you want to delete by performing the procedure described in Section 23.2.3, "Searching for Jobs."

2. Select the jobs from the Search Results table and click the **Delete** button.

   Alternatively, you can select **Delete** from the Actions menu.

   Only the jobs that are not processed can be deleted. The jobs that are processed (finished) contain logs and references to job instances and cannot be deleted. Error messages are displayed when you try to delete these jobs. Processed jobs can only be disabled. Jobs with the In Process status cannot be deleted. If multiple jobs are selected, and if any one of them cannot be deleted, none of the selected jobs will be deleted.

*Table 23–26    Deleting Jobs*

| Status | Can Be Deleted |
|---|---|
| Not Processed | Yes |
| Processed | No. They can only be disabled. |
| In Process | No |

## 23.5.10 Viewing Job Details

Clicking the job name in the Search Results table opens the corresponding Job Details page. The following information is displayed in the Job Details page:

- The General page displays general information about the job such as job type, job name, and job status.

- The Load Details page shows the loader that controls which records will be processed.

- The Rollup Details page shows the monitor rollup details.

- The Run Details page shows the run type details.

- The Data filters tab shows which set of data to load into the offline system or process.

- The Schedule page shows the scheduling options chosen for the job.

## 23.5.11 Viewing Instances of a Job

The Instances tab of the Job Details page shows all past and present job instances for a job. There is a panel at the top that allows the user to filter the job instances shown. The panel at the top allows you to filter the job instances shown.

**Table 23–27    Filter Job Instances**

| Filter | Description |
| --- | --- |
| State | Show only those job instances that are in a particular state, such as Running, Skipped, Completed, or Canceled |
| Process Message | Show only those job instances that match on the process message. |
| Process Start Time | Show only job instances that started processing in the specified timestamp range |
| Process End Time | Show only job instances that stopped processing (whether successfully or unsuccessfully) in the specified timestamp range |

The **Process Now** button allows you to start executing jobs that were skipped or not executed because of errors. If this job is already running and another job of the same job type is already running, you will be informed that this job cannot be started now.

## 23.5.12  Viewing the Job Log

To view the job log, open the Job Log page from the Job Queue page. This page shows past job instances. The top panel allows the user to filter the results.

**Table 23–28    Job Log Filters**

| Filters | Description |
| --- | --- |
| Job Instance Name | Show only job instances that match on job instance name. |
| Job Type | Show only job instances of the specified job type |
| State | Show only those job instances that are in a particular state, such as Running, Skipped, Completed, or Canceled. |
| Process Message | Show only those job instances that match on the process message. |
| Process Start Time | Show only job instances that started processing in the specified timestamp range |
| Process End Time | Show only job instances that stopped processing (whether successfully or unsuccessfully) in the specified timestamp range. |

## 23.5.13  Viewing and Sorting the Job Queue

You can view and sort jobs.

### 23.5.13.1  Viewing the Job Queue

From the Navigation tree, double-click **Job Queue** to open the Job Queue page.

This page shows a listing of currently processing and future jobs. The job instances are displayed in the exact order of execution in the execution queue. There is only one job instance per job.

The recurring job instances have the job name followed by the date and time when the current instance started or the date and time when it will occur next.

The process start time is the exact time when the job started running for current jobs and an estimated start time for the future jobs. Process Duration is shown only for currently processing jobs.

You can filter based on job type, status, start/complete date, name and description. The queue displays which jobs are currently running and what their status is in terms of estimated completion time and percentage progress. Completed jobs will display as such.

The **Job Instance Name** in the table is a link to the Job Details page for the job.

### 23.5.13.2 Sorting the Job Queue

To sort the Job Queue:

1. From the Navigation tree, double-click **Job Queue** to open the Job Queue page.

2. From the Job Queue page, click the Sort Ascending icon on the Priority column or the Start Time column to sort the list.

   Sorting is not allowed on other data points since the job records are placed in the order of execution and this cannot be edited.

   If two jobs have the same start date and time, but different job priority, the higher job priority would be listed first in the Job Queue

## 23.6 Editing Jobs

This section contains instructions to edit jobs.

### 23.6.1 Editing Jobs

The Job Edit page allows you to modify and reschedule a job.

Table 23–29 summarizes the Job Edit tabs.

*Table 23–29    Edit Job*

| Edit Job Tabs | Description |
| --- | --- |
| General | General information for the job: job type, name, and status. The Job Name field cannot be modified. |
| Job Type | The fields on this tab are specific to the job type. |
| Schedule | Similar to Schedule page of the Job Creation wizard. |
| Instances | This tab shows all past and present job instances for a job. |

You can make the following changes:

1. Enable or disable a job from the General tab.

2. Change the Transaction and Memory Buffer Size from the Run Details tab.

3. Change the job schedule from the Schedule tab.

Only the job instance for next occurrence are affected by the edits. The ones that are currently processing are not affected.

### 23.6.2 Editing the Monitor Data Rollup

To edit a Monitor Data Rollup Job, follow these steps:

1. Make the following changes:

   a. Enable or disable a job from the General tab.

   b. Change the Transaction and Memory Buffer Size from the Run Details tab.

   c. Change the job schedule from the Schedule tab.

2. Click the **Process Now** button.

The Monitor Data Rollup Job is processed on a one time basis. The regular schedule of this job is not affected by the one-time job execution. The job will be executed again at its regular scheduled date and time.

## 23.7 Migration

If you are loading from a non-OAAM schema, you must set up the required database view. Refer to "*Creating a View of a Non-OAAM Database*" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

## 23.8 Use Cases

Use cases are presented below.

### 23.8.1 Use Case: Load OAAM Login Data and Run Checkpoints on a Recurring Basis

1.  Security Administrator activates the option to create a new job.

2.  Security Administrator selects the **Load and Run Job** from a dialog.

3.  Security Administrator fills in the general information and clicks **Next**.

4.  Security Administrator is presented with the Load Details page. Security Administrator selects **OAAM Loader**, fills in the Database Connection information, accepts the default Data Mappings, and, if desired, modifies the miscellaneous properties. Security Administrator then clicks **Next**.

5.  Security Administrator is presented with the Run Details page. Security Administrator selects Default Run Type and, if desired, modifies the Run Properties. Security Administrator then clicks **Next**.

6.  Security Administrator is presented with the Data Filters page. Security Administrator selects **Auto Increment** and selects the desired **From Date**.

7.  Security Administrator is presented with the Schedule page of the wizard. The default Schedule Type should be **Once**, and the **Start Date** and **Start Time** should be set to the current date and time by default.

8.  Security Administrator selects the **Recurring** Schedule Type and sets the schedule details to the desired values. Security Administrator may also change the job priority and set the **Cancel Time**, if desired.

9.  Security Administrator clicks **Next**, confirms the information on the Summary, and clicks **Finish**.

**Alternate Courses of Action 1**: If the remote database is not an OAAM schema, then in step 4, the Security Administrator will be required to change the default values for the Data Mappings to match the database schema.

**Alternate Courses of Action 2**: If the data to be loaded is in a file rather than a database, then the Security Administrator may write a custom loader to load the data from the file, but a better practice would be to import the file data into a database table and follow Alternate Courses of Action 1.

**Alternate Courses of Action 3**: The job instance is placed into the Job Queue and is scheduled to start at the desired time. When complete, the next job instance is placed into the Job Queue. The loaded data will be available in the sessions list.

## 23.8.2 Use Case: Load Transaction Data and Run Checkpoints on a Recurring Basis

Pre-conditions: Security Administrator is in OAAM Admin and has the appropriate permissions. A custom loader has been written and the resulting classes have been specified in the OAAM Offline application's classpath. Any needed properties have been set in the OAAM Environment Manager.

1. Security Administrator activates the option to create a new job.

2. Security Administrator selects the **Load and Run Job** Type from a dialog.

3. Security Administrator fills in the general information and clicks **Next**.

4. Security Administrator is presented with the Load Details page. Security Administrator selects **Custom Loader** Type and clicks **Update Class Path**.

5. Security Administrator types in the fully qualified Java class name for the Custom Loader Type and clicks **OK**.

6. Security Administrator modifies the miscellaneous properties if desired and clicks **Next**.

7. Security Administrator is presented with the Run Details page. Security Administrator selects Default Run Type and, if desired, modifies the Run Properties. Security Administrator then clicks **Next**.

8. Security Administrator is presented with the Data Filters page. Security Administrator selects **Auto Increment** and selects the desired **From Date**.

9. Security Administrator is presented with the Schedule page of the wizard. The default Schedule Type should be **Once**, and the **Start Date** and **Start Time** should be set to the current date and time by default.

10. Security Administrator selects the **Recurring** Schedule Type and sets the schedule details to the desired values. Security Administrator may also change the **Job Priority** and set the **Cancel Time**, if desired.

11. Security Administrator clicks **Next**, confirms the information on the Summary, and clicks Finish.

   The job instance is placed into the Job Queue and is scheduled to start at the desired time. When complete, the next job instance is placed into the Job Queue. The loaded data will be available in the sessions list.

**Alternate Courses of Action**: An error will occur at step 5 if there is a problem instantiating the Custom Loader. One possible problem is that the system cannot find the class. Another possible problem is that the class exists, but an error occurred when instantiating the class. The final possible problem is that the system was able to instantiate the class, but it does not properly implement the custom loader specification. The user will receive a different error message depending on the problem.

## 23.8.3 Use Case: Create a Job for Immediate Execution

Preconditions: Security Administrator is in the OAAM Admin Console and has the appropriate permissions.

Actors: Security Administrator

Steps:

1. The Security Administrator activates the option to create a new Job.

2. The Security Administrator selects the desired Job Type from a dialog.

3. The Security Administrator fills in the general information and clicks **Next**.

4. The Security Administrator fills in the Job Type specific information and clicks **Next** (this may be multiple screens, depending on the Job Type).

5. The Security Administrator is presented with the Schedule screen of the wizard. The default Schedule Type should be **Once**, and the Start Date and Start Time should be set to the current date and time by default.

6. The Security Administrator ensures that the Schedule Type is set to **Once** and that the Start Date and Start Time are set to the current date and time. The Security Administrator may also change the Job Priority and set the Suspend Time, if desired.

7. The Security Administrator clicks **Next**, confirms the information on the Summary, and clicks **Finish**.

**Alternate Courses of Action:**

Alternate Courses of Action 1: If the selected Job Type is mutually exclusive, and another Job of the same Job Type is currently executing, this new job will be placed into the Job Queue, but will not begin executing until the currently executing Job is completed.

Post-conditions: The Job begins executing, and the Job Instance is visible in the Job Queue.

### 23.8.4 Use Case: Create a Job for Future Execution

**Preconditions**: The Security Administrator is in the OAAM Admin Console and has the appropriate permissions.

**Actors**: Security Administrator

**Steps**:

1. The Security Administrator activates the option to create a new Job.

2. The Security Administrator selects the desired Job Type from a dialog.

3. The Security Administrator fills in the general information and clicks **Next**.

4. The Security Administrator fills in the Job Type specific information and clicks **Next** (this may be multiple screens, depending on the Job Type).

5. The Security Administrator is presented with the Schedule screen of the wizard. The default Schedule Type should be **Once**, and the Start Date and Start Time should be set to the current date and time by default.

6. The Security Administrator ensures that the Schedule Type is set to **Once**. The Security Administrator sets the Start Date and Start Time to the desired date and time. The Security Administrator may also change the Job Priority and set the Suspend Time, if desired.

7. The Security Administrator clicks **Next**, confirms the information on the Summary, and clicks **Finish**.

**Alternate Courses of Action**: None.

**Post-conditions**: The Job Instance is placed into the Job Queue and is scheduled to start at the desired time.

### 23.8.5  Use Case: Create a Job With Recurring Execution

**Preconditions**: Security Administrator is in the OAAM Admin Console and has the appropriate permissions.

**Actors**: Security Administrator

Steps:

1. The Security Administrator activates the option to create a new Job.

2. The Security Administrator selects the desired Job Type from a dialog.

3. The Security Administrator fills in the general information and clicks **Next**.

4. The Security Administrator fills in the Job Type specific information and clicks Next (this may be multiple screens, depending on the Job Type).

5. The Security Administrator is presented with the Schedule screen of the wizard.

6. The Security Administrator sets the Schedule Type to **Recurring** and sets the Start Date and Start Time to the desired date and time. The Security Administrator may also change the Job Priority and set the End Time and Suspend Time, if desired.

7. The Security Administrator clicks **Next**, confirms the information on the Summary, and clicks **Finish**.

**Alternate Courses of Action**: None.

**Post-conditions**: The Job Instance is placed into the Job Queue and is scheduled to start at the desired time. When complete, the next Job Instance is placed into the Job Queue.

### 23.8.6  Use Case: View the Job Queue

**Preconditions**: Security Administrator is in the OAAM Admin Console and has the appropriate permissions.

**Actors**: Security Administrator

Security Administrator activates the option to display the Job Queue, and clicks the **Current Queue** tab, if necessary.

**Alternate Courses of Action:**

**Alternate Courses of Action 1**: If the Security Administrator wishes to pause a Job Instance, then she will click the desired Job Instance (or multi-select the Job Instances) and click the **Pause** button. The Job Instance will remain in the Job Queue, but the State will be changed to **Paused**. If the Job Instance was executing, it will stop, and if another Job Instance was blocked on this one, it will begin executing.

**Alternate Courses of Action 2**: If the Security Administrator wishes to resume a paused Job Instance, then she will click the desired Job Instance (or multi-select the Job Instances) and click the **Resume** button. If the scheduled start time for this Job Instance has passed and there are no other conflicting Jobs already running, this Job Instance will go into **Running** state and will begin executing. Otherwise this Job Instance will go into **Scheduled** state. If multiple Job Instances are resumed at the same time, then the one with the earliest scheduled start time will go first.

**Alternate Courses of Action 3**: If the Security Administrator wishes to cancel a Job Instance, then she will click the desired Job Instance (or multi-select the Job Instances) and click the **Cancel** button. The selected Job Instance(s) will be removed from the Job Queue. If the Job is recurring, then the next Job Instance will be placed into the Job Queue.

Post-conditions: The system displays all currently executing and upcoming Job Instances. If a Job is recurring, only the next instance is displayed.

### 23.8.7 Use Case: View the Logs from a Job Execution

Preconditions: Security Administrator is in the OAAM Admin Console and has the appropriate permissions.

Actors: Security Administrator

To view the logs from a job execution:

1.  Double click **Job Queue** in the Navigation tree.

2.  Click the **Job Log** tab.

    This page tab past job instances. The top panel allows the user to filter the results.

3.  Search for the Job Instance.

This page shows past job instances. The top panel allows the user to filter the results.

*Table 23–30    Job Log Filters*

| Filters | Description |
| --- | --- |
| Job Instance Name | Show only job instances that match on job instance name. |
| Job Type | Show only job instances of the specified job type |
| Job State | Show only those job instances that are in a particular state, such as Running, Skipped, Completed, or Canceled. |
| Process Message | Show only those job instances that match on the process message. |
| Process Start Time | Show only job instances that started processing in the specified timestamp range |
| Process End Time | Show only job instances that stopped processing (whether successfully or unsuccessfully) in the specified timestamp range. |
| Completed % | The percentage of the job that completed. |
| Process Duration | The time in seconds for completion |

Alternate Courses of Action: None.

Post-conditions: The system displays the filtered list of past Job Instances.

### 23.8.8 Use Case: Check If the Job Ran Successfully

To check if the job ran successfully:

1.  Open the Job Details page of the newly created job.

2.  Click the **Instances** tab to check for job completion.

    If the Run Job schedule time has elapsed, search for the job instance. Its State should be **Completed** with a Process Start Time and a Process End Time. The Process Message should show the number of records processed and the Completed % should show the percentage completed. The Process Duration should show the time in seconds for completion.

3.  Verify job completion by opening to the Sessions page and searching by the same time period as the job.

    For a Run Job, the Count of Sessions should be the same as that of after the load completion. For a Load Job, the Count of Sessions should have increased by the

number shown in the job instances page. For a Load and Run Job, the Count of Sessions should have increased by the number of records processed as shown in the job instance.

4. Open a Session Details page.

For a Run Job and a Load and Run Job, the Sessions details page should show that policies and rules have been processed on the records. For a Load Job, you should see that the record is loaded but no policies and rules have been processed on the session record.

### 23.8.9 Use Case: View the Order of Execution of Jobs

From the Navigation tree, double-click **Job Queue** to open the Job Queue page. This page shows a listing of currently processing and future jobs. The job instances are displayed in the exact order of execution in the execution queue. There is only one job instance per job.

The recurring job instances have the job name followed by the date and time when the current instance started or the date and time when it will occur next.

The process start time is the exact time when the job started running for current jobs and an estimated start time for the future jobs. Process Duration is shown only for currently processing jobs.

You can filter based on job type, status, start/complete date, name and description. The queue displays which jobs are currently running and what their status is in terms of estimated completion time and percentage progress. Completed jobs will display as such.

The **Job Instance Name** in the table is a link to the Job Details page for the job.

# Part IX

## Reporting

This part contains information about reporting features in Oracle Adaptive Access Manager 11*g*.

It contains the following chapters:

- Chapter 24, "Using the Dashboard"
- Chapter 25, "Configuring BI Publisher Reports"
- Chapter 26, "Monitoring Performance by Using Fusion Middleware Control"
- Chapter 27, "Monitor and Audit of Events"

# 24

# Using the Dashboard

The Oracle Adaptive Access Manager Dashboard is an application that provides a high-level view of real monitor data.

This chapter provides detailed instructions on how to use the dashboard to monitor real-time performance and activity. It contains the following topics:

- Introduction
- Using the Dashboard in Oracle Adaptive Access Manager
- Use Cases

## 24.1 Introduction

This section introduces you to the dashboard and how it is used.

### 24.1.1 What is a Dashboard?

The Oracle Adaptive Access Manager Dashboard is an application that provides a high-level view of real monitor data. Monitor data is a representative sample of data.

It presents a real-time view of activity via aggregates and trending.

The Dashboard is comprised of three sections that enable you to focus your review on relevant data, such as the following:

- Performance statistics
- Expanded summary data
- Statistics based on location, scoring, device, security, and performance

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.

The level of access to the dashboard (user interface views and controls) is based according to roles and company requirements.

### 24.1.2 Common Terms and Definitions

This section contains common dashboard terms and definitions.

*Table 24–1    Common Dashboard Terms and Definition*

| Term | Definition |
| --- | --- |
| Refresh | Rate to update Dashboard with new data. The choices are 30 seconds, 1 minute, and 10 minutes. |
| Performance Panel | Section 1 of the Dashboard shows real-time data. |
| Summary Panel | Section 2 of the Dashboard shows aggregate data. |
| Dashboard Panel | Section 3 of the Dashboard shows historical data. |
| Data type | Type of information in the Oracle Adaptive Access Manager system. |
| Range | 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 Transactions | Transactions that were blocked during the transaction checkpoint. |
| High Alert (Logins) | High level alerts triggered during the login checkpoint. |
| High Alert (Transactions) | High level alerts triggered during the transaction checkpoint. |
| KBA Challenges | Challenge question responses. |
| OTP Challenges | OTP challenge responses |

## 24.2 Navigation

From the Navigation tree, double-click **Dashboard**. The Dashboard will appear in OAAM Admin's right side.

The dashboard is divided into three sections:

- The performance panel (Section 1) presents real-time 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 (Section 2) presents aggregate data based on time range and different data types.

- The dashboard panel (Section 3) presents historical data. The detailed dashboards are used for trending data over time ranges.

## 24.3 Using the Dashboard in Oracle Adaptive Access Manager

The Oracle Adaptive Access Manager 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.

### 24.3.1 Performance

This section provides information on viewing the total view and trending views.

#### 24.3.1.1 Viewing Statistics in Total View and Trending View

The Performance panel (Section 1) displays 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.

#### 24.3.1.2 Viewing Performance Data

To view the performance data:

1. Select the data type you want from the **Data** list.

   The data types provided are:

*Table 24–2   Performance Data Types*

| Data Type | Definition |
| --- | --- |
| Logins per minute | Number of successful login per minute |
| KBA challenges per minute | Number of challenge question responses per minute |
| OTP challenges per minute | Number of OTP challenge 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 checkpoint per minute |
| High Alert (Transactions) per minute | Number of high alerts triggered during the transaction checkpoint 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, select the refresh rate from the **Refresh** list.

*Figure 24–1 Performance Panel*



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.

### 24.3.1.3 Difference Between Performance Panel and Performance Dashboard

The Performance panel (Section 1) 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.

The Performance dashboard is one of the five detailed dashboards in Section 3. Section 3 provides accurate totals and trends them over time.

A good analogy to the difference between these two views is a speedometer. Section 1 is like 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. If Section 1 shows the rate at which you are traveling, Section 3 shows your actual distance traveled.

## 24.3.2 Summary

The Summary panel displays an overview or aggregate of the selected data type for the specified range or time fame.

### Data Types

Table 24–3 presents the data types in the Summary panel.

*Table 24–3 Summary Data Types*

| Data Type | Definition |
| --- | --- |
| Login Sessions | Login sessions |
| Success Logins | Successful logins |
| Temporary Allow Logins | Logins that occurred while a temporary allow was active |
| Blocked Logins | Logins that were blocked during the login checkpoint |
| High Alert (Logins) | High level alerts triggered during the login checkpoint |
| KBA Challenges | Challenge question responses |
| OTP Challenges | OTP challenge responses |
| Transaction Sessions | Transaction ID |
| Success Transactions | Successful transactions |

*Table 24–3   (Cont.)  Summary Data Types*

| Data Type | Definition |
| --- | --- |
| Blocked Transactions | Transactions that were blocked during the transaction checkpoint. |
| High Alert (Transactions) | High level alerts triggered during the transaction checkpoint |
| Average Rule Process Time | Average number of milliseconds for rule execution |
| Average Policy Process Time | Average number of milliseconds for policy execution |
| Average Checkpoint Process Time | Average number of milliseconds for checkpoint 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.

*Figure 24–2   Summary panel*



**Refresh**

To change the refresh rate, click the **Refresh** list and then click the refresh rate you want.

**Range**

To change the range or timeframe, click the **Range** list and then click the range you want.

## 24.3.3  Dashboards

Section 3 provides access to five different dashboard types:

- Location

  For information about the Location dashboard, refer to Section 24.3.3.1, "Viewing Data Type by Location."

- Scoring

  For information about the Scoring dashboard, refer to Section 24.3.3.2, "Viewing a List of Scoring Breakdowns."

- Security

  For information about the Security dashboard, refer to Section 24.3.3.3, "Security Dashboard," and Section 24.3.3.4, "Viewing a List of Rules or Alerts by Security."

- Device

For information about the Device dashboard, refer to Section 24.3.3.5, "Viewing Browser and Operating System Data by Device."

■ Performance

For information about the Performance dashboard, refer to Section 24.3.3.6, "Viewing a Data Type by Performance."

*Figure 24–3   Five Dashboards*
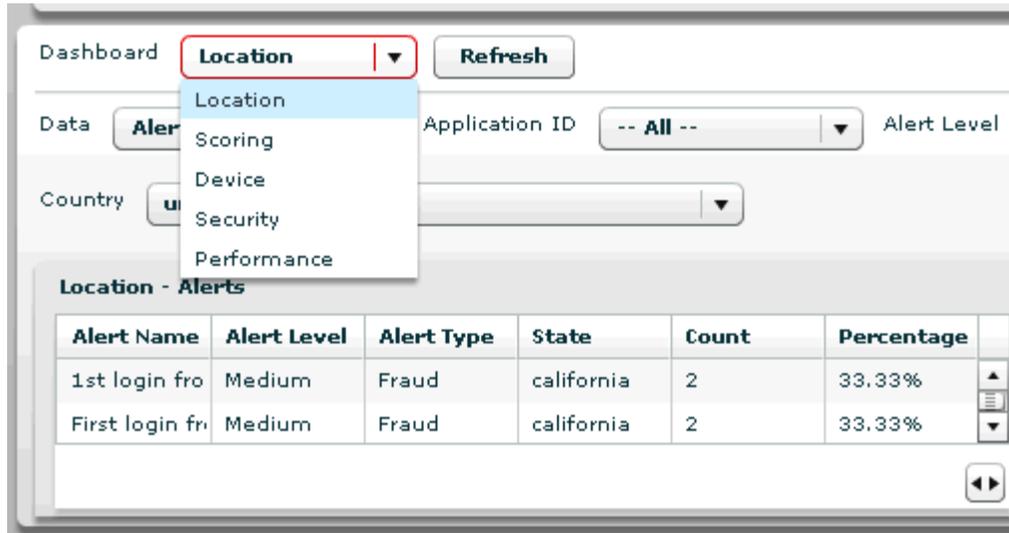


For each dashboard type you can select the type of data you want to see from a menu of data types. For example, if you select the **Location** dashboard, a **Country** list appears that enables you to select the country you want.

*Figure 24–4   Choices After Data Type Selection*
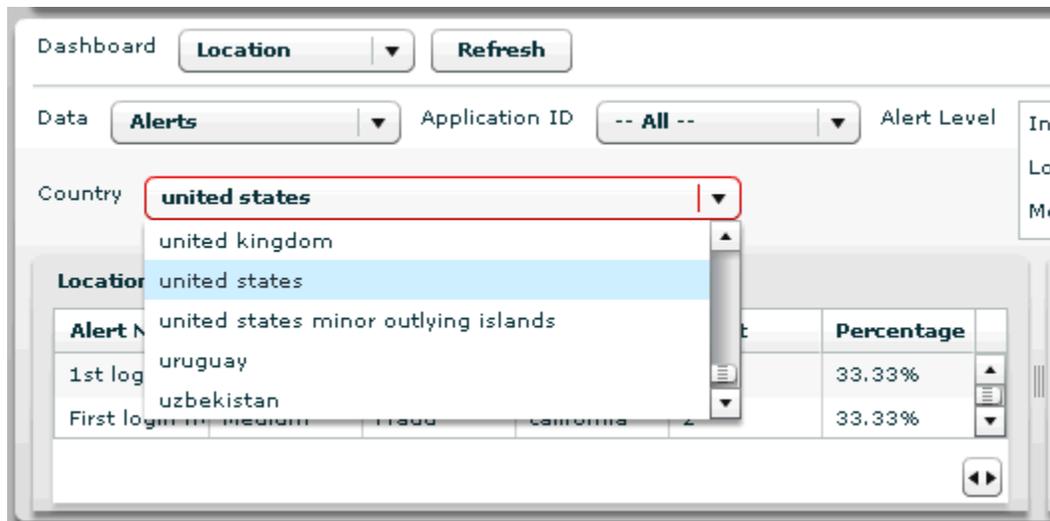
### 24.3.3.1 Viewing Data Type by Location

You can view data type by location.

1. In Section 3, in the **Dashboard** drop-down menu, select **Location**.

   The section becomes a Location dashboard.

2. In the **Data** drop-down menu, select the data type you want to view by location.

   The data types you can select to view by country are the following:

*Table 24–4    Data Types by Location*

| Data Types by Location | Definition |
| --- | --- |
| Alerts | Alert that have been triggered by country |
| Actions | Actions that have been taken by country |
| KBA Challenges | KBA challenges that have been triggered by challenge result and country |
| OTP Challenges | OTP challenges that have been triggered by challenge result and country |
| Routing Type | Routing types by country |
| Sessions | Sessions by country |
| Temporary Allow | Temporary allows that have been made by country |

3. To narrow the list to a specific **Organization ID**, select an application from the **Organization ID** drop-down menu

4. To narrow the list to a specific timeframe, select a ranges from the **Range** drop-down menu.

5. To narrow the list to a specific checkpoint, select a checkpoint from the **Checkpoint** drop-down menu.

6. To narrow the list to a specific country, select a country from the **Country** list, click the country you want.

7. 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.

8. If you selected the alerts or temporary allow data type, you can narrow the list further by selecting the checkpoint you want from the **Checkpoint** 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.

### 24.3.3.2 Viewing a List of Scoring Breakdowns

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 checkpoint, in the **Checkpoint** list, click the Checkpoint you want.

3. To narrow the list to a specific timeframe, in the **Ranges** list, click the range you want.

4. Click **Refresh**.

### 24.3.3.3 Security Dashboard

Items in the Dashboard list are accessible based on your role. Only fraud investigators can access the Security dashboard.

### 24.3.3.4 Viewing a List of Rules or Alerts by Security

To view a list of rules 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 **Organization ID**, on the **Organization ID** list, click the **Organization ID** you want.

4. To narrow the list to a specific checkpoint, in the **Checkpoint** 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**.

### 24.3.3.5 Viewing Browser and Operating System Data by Device

To view 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 **Organization ID**, in the **Organization ID** list, click the Organization ID you want.

3. To narrow the list to a specific timeframe, in the **Ranges** list, click the range you want.

4. Click **Refresh**.

### 24.3.3.6 Viewing a Data Type by Performance

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:

*Table 24–5    Data Type by Performance*

| Data Type by Performance | Definition |
| --- | --- |
| Rules | Rules currently in the system |
| Policies | Policies currently in the system |
| Checkpoints | 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 Cases subsystem |
| Rules APIs | Calls to the rules processor |

*Figure 24–5    Viewing Data Type by Performance*



3. If you selected the rules or policies data type, you can narrow the list further by selecting the checkpoint you want from the **Checkpoint** list.

4. To view data trended over a specific timeframe, in the **Ranges** list, click the range you want.

5. To trend data for a specific data type item, select the row from the **Performance** table.

6. Click **Refresh**.

### 24.3.3.7  Using the Total and Trending Views

The left side of the dashboard panel displays a total view and the right side displays a trending view of the selected data type.

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.

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.

**Figure 24–6   Total and trending views**
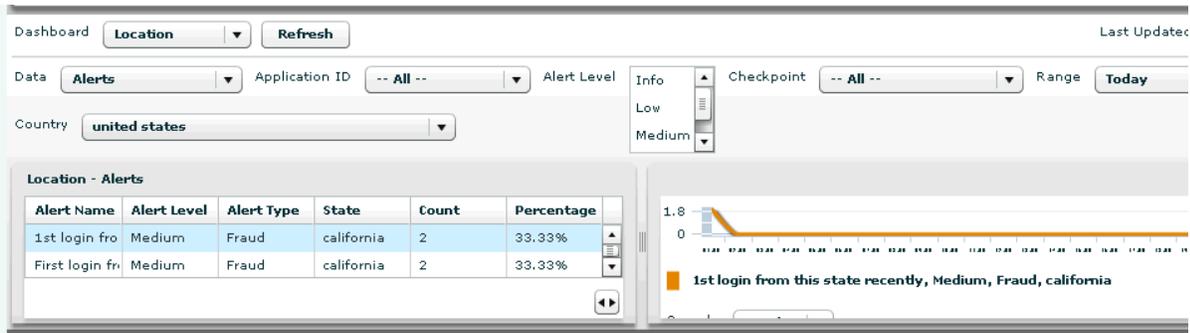


### 24.3.3.8  Viewing the Trending View Graph

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.

### 24.3.3.9  View by Range

To narrow the data gathered to a specific time frame, from the **Range** list, select Today, Last 1 day, Last 7 days, Last 30 days, or Last 90 days.

### 24.3.3.10  View by Sample

To view data by a periodic interval, from the **Samples** list, select hourly, daily, weekly, or monthly. The choices available will depend on the range selected.

An example would be that if you have collected data over a period of six months, and you want to show how much data was collected every day using last month's data, you would choose to show daily samples trended over a month.

### 24.3.3.11  Last Updated

The "Last Updated" field, which also appears in the performance panel (Section 1), is updated when you select a different data type.

### 24.3.3.12  Using Tooltips

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.

*Figure 24–7 Tooltips*
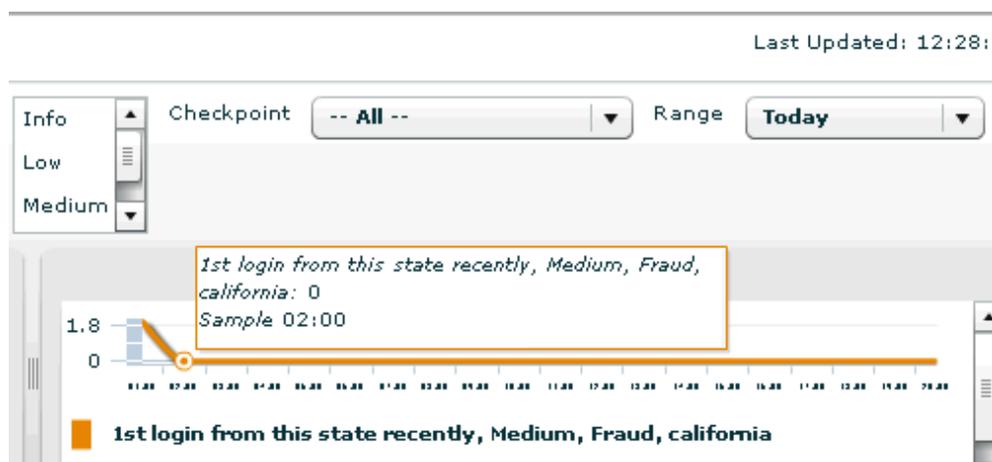


## 24.4 Use Cases

This section provides a scenario of how Oracle Adaptive Access Manager's dashboards are used.

### 24.4.1 Use Case: Trend Rules Performance on Dashboard

Through using the dashboard, Security Administrators--who plan, configure and deploy policies--can monitor the performance of rules and modify if necessary.

Rules and policies can potentially have a performance impact. For example, if the Security Administrator defines a new policy to check for a user, who is not using an email address that had been used before (ever). If the bank has more than 1 billion records in the database, performing that check against all the records for every transaction has great impact on performance.

To trend rule performance on the dashboard (find the average rule processing times for the past week with daily samples):

1.  Log in to OAAM Admin.

2.  In the Navigation tree, select **Dashboard**. The dashboard is displayed.

    The dashboard is divided into three sections:

    ■   The **performance panel** on the top presents real-time 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** at the bottom presents historical data. The detailed dashboards are used for trending data over time ranges.

3.  In the performance dashboard in Section 3, select **Performance** from the Dashboard list.

4.  Select **Rules** from the Data list.

    You have selected **Rules** to view rule performance.

    The rules appear in the **Performance - Rules** table.

5. Narrow the data to view by a specific time frame. To view average rule processing times for the past week, in the **Range** list, select **Last 7 Days**.

   The average processing time for each rule is shown in the **Average Processing Time** column of the **Performance-Rules** table.

6. Select the sample to use to trend the data. To specify that you want to use daily samples to trend the performance data, select **Daily** from the **Sample** list.

7. View the specific trend graph. Click a specific rule in the **Performance - Rules** table to see the performance trend graph.

## 24.4.2 Use Case: View Current Activity

Business Analyst, Security Administrators, and Fraud Investigators are interested in actions that affect the user.

The Dashboard panel (Section 3) displays a total view and a trending view of the selected data type.

To monitor actions:

1. View the number of blocks

2. View the number of KBA challenges

3. View the number of OTP challenges

4. Trend the information over time, taking note of spikes and number of customers affected.

## 24.4.3 Use Case: View Aggregate Data

Business Analyst, Security Administrators, and Fraud Investigators are interested in actions that affect the user.

To obtain up-to-date numbers for user access and actions, view the Summary panel (Section 2), which provide an aggregate of the data.

## 24.4.4 Use Cases: Additional Security Administrator and Fraud Investigator Use Cases

Security Administrators and Fraud Investigators are interested in viewing:

- Current activity and trended activity over time

- Average performance numbers and trended performance averages over time

- Distribution of events trended by geography

- Security events trended over time

**Viewing Current Activity and Trended Over Time**

Security Administrators and Fraud Investigators are interested in viewing current activity and trended over a short period of time.

1. Log in to OAAM Admin.

2. Navigate to the Dashboard.

3. In the Performance Panel (Section 1) select a data type from the **Data** list.

4. View statistics in total view and trending view.

   - Total view - current activity over short period of time

- Trending view - current activity trended over a short period of time

5. In the Summary Panel (Section 2), view a summary of the current activity for a range.

   - Sessions

   - Actions

   - Alerts

   - and others

### Average Performance Numbers and Trended Performance Averages Over Time

Security Administrators and Fraud Investigators are interested in viewing average performance numbers and trended performance averages over time

1. Log in to OAAM Admin.

2. Navigate to the **Dashboard**.

3. In the Performance dashboard (in Section 3), view the following by performance.

   - Rules

   - APIs

   - and others

### Distribution of Events Trended by Geography

Security Administrators and Fraud Investigators are interested in viewing a distribution of events trended by geography.

1. Log in to OAAM Admin.

2. Navigate to the **Dashboard**.

3. In the Performance dashboard (in Section 3), view events by location.

   - Sessions

   - Actions

   - Alerts

   - and others

### Security Events Trended Over Time

Security Administrators and Fraud Investigators are interested in viewing security events trended over time.

1. Log in to OAAM Admin.

2. Navigate to the **Dashboard**.

3. In the Performance dashboard (in Section 3), view security events.

   - Rules

   - Alerts

   - and others

### 24.4.5  Use Cases Additional Business Analyst Use Cases

Business Analyst are interested in viewing:

- Customer behavior trend
    - Operating system browser combinations
    - KBA challenges
    - Blocks
- Distribution of events trended by geography
    - sessions
    - actions
    - alerts
    - and so on

### 24.4.6  Use Case: Viewing OTP Performance Data

1. In the Navigation tree, double-click **Dashboard**.

2. Check Section I of the **Dashboard** for **OTP Challenges per minute**.

   The graph displays the **OTP Challenges per minute** statistics

3. Check Section II of the Dashboard

   The summary table of the Dashboard displays the **Count of OTP Challenges** for the specified time period.

4. Check Section III of the Dashboard under **Locations**.

   The **Location Dashboard** displays performance statistics, such as **count**, **percentage**, and others.

# 25

# Configuring BI Publisher Reports

This chapter describes how to configure reporting and how to view Oracle Adaptive Access Manager reports. It contains these topics:

- Oracle Business Intelligence Publisher Reports
- Investigation and Forensics
- Setting up Oracle Business Intelligence Publisher for Oracle Adaptive Access Manager Reports
- Setting Preferences
- BI Publisher's Users, Roles, and Permissions
- Scheduling a Report
- Viewing/Running Reports
- Building OAAM Transactions Reports
- Adding Translations for the BI Publisher Catalog and Reports
- Use Cases

## 25.1 Oracle Business Intelligence Publisher Reports

Oracle Adaptive Access Manager utilizes Business Intelligence Publisher for the majority of reporting functions. All OAAM customers are recommended to replicate production data into a reporting database and to provide a dedicated reporting environment for BI Publisher.

Oracle BI Publisher is an Oracle's enterprise reporting solution and provides a single reporting environment to author, manage, and deliver all of your reports and business documents. Utilizing a set of familiar desktop tools, such as Microsoft Word, Microsoft Excel, or Adobe Acrobat, you can create and maintain report layouts based on data from diverse sources, including Oracle Identity Management products.

## 25.2 Investigation and Forensics

Oracle Adaptive Access Manager provides access to a rich set of forensic data to power investigations and auditing. Business Intelligence Publisher provides the reporting engine allowing reporting to be fully customized to meet requirements. Out of the box report templates are included that can be used as is or altered. The intuitive administration console interface makes it quick and easy to narrow in on the important data and relationships. This allows a security analyst to find related situations that otherwise might not be identified and better understand the

relationships between various security events. Oracle Adaptive Access Manager leverages the common audit framework from Oracle Platform Security Services to capture full audit trails for administration console users.

## 25.2.1 Session Activity Aggregates

BI Publisher reports can be used to show the results of checkpoints.

- Total number of each action by checkpoint

- Total number of each alert by checkpoint

- Total number of sessions with risk score ranges (0 - 600, 601 - 800, 801 - 1000) by checkpoint

### Login Analysis Aggregates Report

For example, George is a security and compliance officer. He has been asked to configure a solution to run login risk evaluations offline that are deemed too expensive to run in real-time. He is using the out of the box run task to perform the whole login chain of checkpoints on every session in the selection. After the load and run are complete George generates an aggregate report showing metrics for total numbers of each action, alert, risk scores in pre-auth and post-auth data.

For example, George is a security and compliance officer. He has been asked to configure a solution to run login risk evaluations offline to test new policies before they are rolled out to production. When testing to see the difference in results between one policy configuration and another he performs a run with policy set A then he runs this report and exports to HTML. Next he does the same with policy set B and compares the two reports to see if policy changes are behaving as expected.

## 25.2.2 Search Sessions By Case Disposition

As Investigation Managers and business analysts, you can assess the effectiveness of OAAM and your fraud team. As part of investigating, you can run a report that returns all sessions that have been linked to a case with a specified disposition. The results will show the case IDs each session is linked to.

### Search sessions by case disposition Report

At the end of the week a manager runs the report to find a list of all sessions with organization ID "Sears" and that have been linked to a case with a "confirmed fraud" disposition.

## 25.2.3 Audit

In Oracle Fusion Middleware 11*g* Release 1 (11.1.1), auditing provides a measure of accountability and answers to the "who has done what and when" types of questions.

Audit is used for tracking OAAM Admin operations, such as creating policy, deleting group, and so on. OAAM collects audit information and it is sent to the audit database. The user can view audit data through BI Publisher, which reads the audit database. You can control the audit functionality through Enterprise Manager where you can choose which events to audit, key in users to always audit, or audit only failure events. So Audit involves: EM (audit setting), OAAM (audit event generation), BI (audit report viewing). For information on setting up audit data sources, refer to "Configuring and Managing Auditing" in the *Oracle Fusion Middleware Application Security Guide*. For information on setting up Oracle Business Intelligence Publisher for

use with audit reports, refer to "Using Audit Analysis and Reporting" in the *Oracle Fusion Middleware Application Security Guide*.

## 25.3 Setting up Oracle Business Intelligence Publisher for Oracle Adaptive Access Manager Reports

When your data resides in a database, you can run pre-defined Oracle Business Intelligence Publisher (BI Publisher) reports and create your own reports on the data. This section contains these topics about configuring your environment for reports:

- Installing BI Publisher
- Installing Oracle Adaptive Access Manager BI Publisher Reports
- Configuring Oracle Adaptive Access Manager BI Publisher Reports

### 25.3.1 Installing BI Publisher

OAAM uses Oracle BI Publisher to generate your OAAM reports.

Perform the following steps to acquire and install Oracle BI Publisher:

1. Go to Oracle Technology Network web site at
   http://www.oracle.com/technetwork/index.html

2. Locate the Oracle BI Publisher Download page by searching on the key words Oracle BI Publisher or Oracle BI Publisher Download.

3. Review the Oracle Technology Network License Agreement that appears on the Oracle BI Publisher Download page. You must accept the Oracle Technology Network License Agreement to download Oracle BI Publisher.

4. Download the version of Oracle BI Publisher that is appropriate for your operating system by clicking on the appropriate link.

5. Install Oracle BI Publisher by referring to the Oracle Business Intelligence Publisher Installation Guide. Refer to Oracle Business Intelligence Publisher Documentation for information about accessing the Oracle Business Intelligence Publisher Installation Guide.

6. Verify your Oracle BI Publisher is operational before installing and configuring the OAAM reports.

### 25.3.2 Installing Oracle Adaptive Access Manager BI Publisher Reports

This section explains how to install BI Publisher Reports. You must install Oracle BI Publisher and verify it is operational before installing the BI Publisher Reports. Refer to Oracle Business Intelligence Publisher Documentation if you need more information.

Perform the following steps to install the reports:

1. Stop the Oracle BI Publisher server. Refer to Oracle Business Intelligence Publisher Documentation if you need more information.

2. On your OAAM host, locate the OAAM products reports package from the `/IAM_HOME/oaam/reports` directory and extract the contents to a location on your Oracle BI Publisher server. For example:

   /ORACLE_BI_PUBLISHER_HOME/xmlp/XMLP/reports

3. Copy the `properties.xml` file to any directory in Oracle BI Publisher server's file system.

4. Start the Oracle BI Publisher server. Refer to Oracle Business Intelligence Publisher Documentation if you need more information.

### 25.3.3 Configuring Oracle Adaptive Access Manager BI Publisher Reports

Perform the following steps to configure the Oracle Adaptive Access Manager reports:

1. Configure the JDBC Data Source for Oracle Adaptive Access Manager by performing the following steps:

   a. Log in to Oracle BI Publisher from a web browser as an Administrator. Refer to Oracle Business Intelligence Publisher Documentation if you need more information.

   b. Click the **Admin** tab, then click **JDBC Connection** under Data Source, and then click the **Add Data Source** button. The Add Data Source screen appears.

   c. Enter the following information in the fields on the Add Data Source screen. Replace the *variable values* in the following examples with the actual values for your Oracle Adaptive Access Manager database.

| Field | Data to Enter |
|---|---|
| Data Source Name | ARM |
| | For the Oracle Adaptive Access Manager reports to work out-of-the-box, the JDBC data source must be named as "ARM". If you choose a different name, you must modify the data source property in all reports. |
| Connection String | `jdbc:oracle:thin:@host:port:sid` |
| User Name | User name for a database schema user that has access to Oracle Adaptive Access Manager. |
| Password | Password for user identified in the User Name field. |
| Database Driver Class | `oracle.jdbc.driver.OracleDriver` |

2. Configure AdminProperties Data Source for Oracle Adaptive Access Manager by performing Steps a and b. The AdminProperties contains configuration information that Oracle Adaptive Access Manager will need to read when generating the reports.

   a. Click the **Admin** tab, then click **File** under Data Source, and then click the **Add Data Source** button. The Add Data Source screen appears.

   b. Enter the following information in the fields on the Add Data Source screen:

| Field | Data to Enter |
|---|---|
| Data Source Name | AdminProperties |
| | You must name this Data Source `AdminProperties`. |
| Full Path of Top-level Directory | Path must be the directory where you placed `properties.xml`. |

The configuration for Oracle Adaptive Access Manager reports is complete. Refer to Oracle Business Intelligence Publisher Documentation if you need more information.

### 25.3.4 Testing Oracle Adaptive Access Manager BI Publisher Configuration

Perform the following steps to test whether the configuration of the Oracle Adaptive Access Manager reports has been successful:

1. Log in to Oracle BI Publisher using a URL of the form:

   `http://host.domain.com:port/xmlserver/`

2. On the main page, click **OAAM** under Shared Folders and then **oradb**.

   The Oracle Adaptive Access Manager reports are now available.

3. Select any report.

4. Select any output type and click the **View** button.

## 25.4 Setting Preferences

You can set the Report Locale, User Interface Language, Time Zone, and Accessibility Mode for BI Publisher.

- Report Locale- A locale is a language and territory combination (for example, English (United States) or French (Canada)). BI Publisher uses the report locale selection to determine the template translation to apply, the number formatting and date formatting to apply to the report data.

- User Interface Language- The User Interface language is the language that your user interface displays in. The language that you selected at login will be selected as the default. However, you can choose from the languages that are available for your installation through this option.

- Time Zone - Select the time zone to apply to your reports. Reports run by you (this user) will display the time according to the time zone preference selected here.

- Accessibility Mode- Setting this to "On" will display the report catalog in a tree structure that is accessible via keyboard strokes

For more information on setting preferences, refer to the "Setting My Account Preferences and Viewing My Groups" chapter of the *Oracle Fusion Middleware Report Designer's Guide for Oracle Business Intelligence Publisher*.

## 25.5 BI Publisher's Users, Roles, and Permissions

In BI Publisher, a user is assigned one or multiple Roles. A Role can grant any or all of the following:

- privileges to use functionality

- permissions to perform actions on catalog objects

- access to data sources

For information on setting users, roles, and permissions, refer to the "Alternative Security Options" chapter of the *Oracle Fusion Middleware Administrator's and Developer's Guide for Oracle Business Intelligence Publisher*.

## 25.6 Scheduling a Report

Oracle BI Publisher Enterprise enables you to schedule reports, and deliver the executed output to various destinations. BI Publisher Scheduler is configured as a part

of Oracle BI Enterprise Edition installation process. Ensure that the scheduler is configured properly, before you start scheduling the reports.

For information on scheduling reports, refer to "Creating Report Jobs" in the *Oracle Fusion Middleware Report Designer's Guide for Oracle Business Intelligence Publisher*.

## 25.7 Viewing/Running Reports

This section explains how to view/run reports.

Take these steps to view/run a report:

1. Log in to Oracle BI Publisher using a URL of the form:

   `http://host.domain.com:port/xmlserver/`

2. On the main page, click **OAAM** under Shared Folders and then **oradb**.

3. Navigate to the report of interest.

   The report is displayed.

4. The report display page contains these major areas:

   - Filters at the top of the page enable you to determine the records to include in the report.

   - Format control buttons enable you to determine:

     – the template type, which can be:

       HTML - This is the default display format.

       PDF - Displays a printable PDF view.

       RTF - Displays a document in Rich Text Format.

       Excel2000 - Displays a spreadsheet.

       Data - Displays an unformatted XML data set.

       To change the template type while viewing a report, select the type from the list and click **View**.

     – output format

     – delivery options

     – range in which to view the data

5. View, save or export the report as desired.

## 25.8 Create Oracle BI Publisher Reports on Data in the OAAM Schema

This section contains instructions on creating Oracle BI Publisher reports on data in the OAAM schema.

In code listings OAAM table and field names are bold and italic.

### 25.8.1 Create a Data Model

Refer to the instructions in *Creating a New Report in the Oracle Business Intelligence Publisher Report Designer's Guide*.

## 25.8.2 Map User Defined Enum Numeric Type Codes to Readable Names

Several fields in many tables are numeric type codes, which correspond to OAAM User Defined Enums. Refer to the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager* for more information about OAAM User Defined Enums. Information on how to map those type codes to readable names is presented in this section.

There are two methods for resolving these names, and the one to choose depends on whether you need to display English only or you need to display internationalized strings.

### 25.8.2.1 Results Display

To display a readable string rather than a type code value in the report output, the report writer will need to add a join to the tables that hold the User Defined Enums, and then add the field to the select clause.

### 25.8.2.2 English Only User Defined Enum Result Display

The following SQL code shows how to add the join criteria to the query:

```
SELECT …
FROM …
LEFT OUTER JOIN (
      SELECT enumElement.num_value, enumElement.label
      FROM v_b_enum enum
            INNER JOIN v_b_enum_elmnt enumElement ON on enum.enum_id = enum_
element.enum_id
      WHERE enum.prop_name = 'enum name') alias
      ON table.type_field = alias.num_value
…
```

In this code, table.type_field is the field containing a type code value that you want to replace with a string. Alias is the name you are giving the inner select clause. Finally, enum_name is the property name of the User Defined Enum.

To display in the report, you need to add *alias*.label to the select clause.

### 25.8.2.3 Internationalized User Defined Enum Result Display

The following SQL code shows how to add the join criteria to the query:

```
SELECT …
FROM …
LEFT OUTER JOIN (
      SELECT t0.config_value, element.num_value
      FROM v_b_config_rb t0
      INNER JOIN (
            SELECT enum_element.num_value, enum_element.str_value, enum.prop_name
            FROM v_b_enum enum
                  INNER JOIN v_b_enum_elmnt enum_element ON enum.enum_id = enum_
element.enum_id
            WHERE enum.prop_name = 'enum name') element
            ON t0.config_name=element.prop_name || '.' || element.str_value ||
'.name'
      WHERE t0.locale_id = (
            SELECT locale_id FROM v_b_locale
            WHERE language = substr(:xdo_user_ui_locale, 1, 2)
                  AND country = substr(:xdo_user_ui_locale, 4, 2)
                  AND (substr(:xdo_user_ui_locale, 1, 2) in ('de', 'en', 'es',
'fr', 'it', 'ja', 'ko')
```

```
                                      OR (substr(:xdo_user_ui_locale, 1, 2) = 'pt' AND
substr(:xdo_user_ui_locale, 4, 2) = 'BR')
                                      OR (substr(:xdo_user_ui_locale, 1, 2) = 'zh' AND
substr(:xdo_user_ui_locale, 4, 2) IN ('CN', 'TW')))
              UNION SELECT locale_id FROM v_b_locale
              WHERE language = substr(:xdo_user_ui_locale, 1, 2)
                    AND NOT EXISTS(SELECT locale_id FROM v_b_locale
                    WHERE language = substr(:xdo_user_ui_locale, 1, 2)
                          AND country = substr(:xdo_user_ui_locale, 4, 2))
                          AND country IS NULL
                          AND (substr(:xdo_user_ui_locale, 1, 2) in ('de', 'en',
'es', 'fr', 'it', 'ja', 'ko')
                                      OR (substr(:xdo_user_ui_locale, 1, 2) = 'pt' AND
substr(:xdo_user_ui_locale, 4, 2) = 'BR')
                                      OR (substr(:xdo_user_ui_locale, 1, 2) = 'zh' AND
substr(:xdo_user_ui_locale, 4, 2) IN ('CN', 'TW')))
              UNION SELECT locale_id FROM v_b_locale
              WHERE language = 'en'
                    AND NOT (substr(:xdo_user_ui_locale, 1, 2) in ('de', 'en',
'es', 'fr', 'it', 'ja', 'ko')
                                      OR (substr(:xdo_user_ui_locale, 1, 2) = 'pt' AND
substr(:xdo_user_ui_locale, 4, 2) = 'BR')
                                      OR (substr(:xdo_user_ui_locale, 1, 2) = 'zh' AND
substr(:xdo_user_ui_locale, 4, 2) IN ('CN', 'TW'))))
      ORDER BY t0.config_name) alias
      ON table.type_field = alias.num_value
…
```

In this code, table.type_field is the field containing a type code value that you want to replace with a string. Alias is the name you want to give the inner select clause. Finally, enum_name is the property name of the User Defined Enum.

To display in the report, you need to add *alias*.config_value to the select clause.

## 25.8.3  Adding Lists of Values

Add parameters to your report definition to enable your users to interact with the report and specify the data of interest from the data set.

To allow a user to select from a list of readable strings representing type codes, the report writer will need to create a List of Values (LOV) from a query on the User Defined Enums tables, filtered by the enum name.

### 25.8.3.1  User Defined Enums as List of Values for Filtering, English Only

The following listing shows how to write the query to populate the list of values.

```
SELECT enumElement.label, enumElement.num_value
FROM v_b_enum enum
      INNER JOIN v_b_enum_elmnt enumElement ON on enum.enum_id = enumElement.enum_
id
WHERE enum.prop_name = 'enum name'
ORDER BY enumElement.label
```

The following listing shows how to filter the report based on this LOV.

```
WHERE …
AND (:parameter IS NULL OR :parameter = table.type_field)
```

In these listings, enum_name is the property name of the User Defined Enum, table.type_field is the field containing a type code value that you want to replace with

a string, and parameter is the named parameter. Review the *Oracle BI Publisher User's Guide* for information about creating and setting up report parameters.

### 25.8.3.2 User Defined Enums as List of Values for Filtering, Internalized

The following listing shows how to write the query to populate the list of values.

```
SELECT t0.config_value, element.num_value
FROM v_b_config_rb t0
INNER JOIN (
      SELECT enum_element.num_value, enum_element.str_value, enum.prop_name
      FROM v_b_enum enum
            INNER JOIN v_b_enum_elmnt enum_element ON enum.enum_id = enum_
element.enum_id
      WHERE enum.prop_name = 'enum name') element
      ON t0.config_name=element.prop_name || '.' || element.str_value || '.name'
WHERE t0.locale_id = (
      SELECT locale_id FROM v_b_locale
      WHERE language = substr(:xdo_user_ui_locale, 1, 2)
            AND country = substr(:xdo_user_ui_locale, 4, 2)
            AND (substr(:xdo_user_ui_locale, 1, 2) in ('de', 'en', 'es', 'fr',
'it', 'ja', 'ko')
                  OR (substr(:xdo_user_ui_locale, 1, 2) = 'pt' AND substr(:xdo_
user_ui_locale, 4, 2) = 'BR')
                  OR (substr(:xdo_user_ui_locale, 1, 2) = 'zh' AND substr(:xdo_
user_ui_locale, 4, 2) IN ('CN', 'TW')))
      UNION SELECT locale_id FROM v_b_locale
      WHERE language = substr(:xdo_user_ui_locale, 1, 2)
            AND NOT EXISTS(SELECT locale_id FROM v_b_locale
            WHERE language = substr(:xdo_user_ui_locale, 1, 2)
                  AND country = substr(:xdo_user_ui_locale, 4, 2))
                  AND country IS NULL
                  AND (substr(:xdo_user_ui_locale, 1, 2) in ('de', 'en', 'es',
'fr', 'it', 'ja', 'ko')
                        OR (substr(:xdo_user_ui_locale, 1, 2) = 'pt' AND
substr(:xdo_user_ui_locale, 4, 2) = 'BR')
                        OR (substr(:xdo_user_ui_locale, 1, 2) = 'zh' AND
substr(:xdo_user_ui_locale, 4, 2) IN ('CN', 'TW')))
      UNION SELECT locale_id FROM v_b_locale
      WHERE language = 'en'
            AND NOT (substr(:xdo_user_ui_locale, 1, 2) in ('de', 'en', 'es',
'fr', 'it', 'ja', 'ko')
                  OR (substr(:xdo_user_ui_locale, 1, 2) = 'pt' AND substr(:xdo_
user_ui_locale, 4, 2) = 'BR')
                  OR (substr(:xdo_user_ui_locale, 1, 2) = 'zh' AND substr(:xdo_
user_ui_locale, 4, 2) IN ('CN', 'TW'))))
ORDER BY t0.config_name
```

The filtering is done in the same manner as the English Only version.

## 25.8.4 Adding Geolocation Data

The OAAM schema includes tables that map IP address ranges to location data including city, state, and country. The relevant tables are VCRYPT_IP_LOCATION_MAP, VCRYPT_CITY, VCRYPT_STATE, and VCRYPT_COUNTRY. Many tables contain IP addresses, and VCRYPT_IP_LOCATION_MAP contains foreign keys to each of VCRYPT_CITY, VCRYPT_STATE, and VCRYPT_COUNTRY.

In OAAM, IP addresses are stored as long numerals. The following listing shows how join a table containing an IP address to the VCRYPT_IP_LOCATION_MAP.

```
SELECT ...
FROM vcrypt_tracker_usernode_logs logs
      INNER JOIN vcrypt_ip_location_map loc ON (
            logs.remote_ip_addr >= loc.from_ip_addr AND logs.remote_ip_addr <=
loc.from_ip_addr
      )
```

For user input and display purposes, you will normally want to use the standard four-part IP address. The following listing shows how to display a numeric IP address as a standard IP, where *ipField* is the field or parameter containing the numeric IP address you want to display.

```
…
to_char(to_number(substr(to_char(ipField, 'XXXXXXXX'), 1, 3), 'XX')) || '.' ||
      to_char(to_number(substr(to_char(ipField, 'XXXXXXXX'), 4, 2), 'XX')) || '.'
||
      to_char(to_number(substr(to_char(ipField, 'XXXXXXXX'), 6, 2), 'XX')) || '.'
||
      to_char(to_number(substr(to_char(ipField, 'XXXXXXXX'), 8, 2), 'XX'))
...
```

The following listing shows how to convert a standard IP address to the long numeric format.

```
…
to_number(substr(ipField, 1, instr(ipField, '.')-1))*16777216 +
      to_number(substr(ipField, instr(ipField, '.', 1, 1)+1, instr(ipField, '.',
1, 2)-instr(ipField, '.', 1, 1)-1))*65536 +
      to_number(substr(ipField, instr(ipField, '.', 1, 2)+1, instr(ipField, '.',
1, 3)-instr(ipField, '.', 1, 2)-1))*256 +
      to_number(substr(ipField, instr(ipField, '.', 1, 3)+1))
```

## 25.8.5  Adding Sessions and Alerts

Sessions and alerts exist in the VCRYPT_TRACKER_USERNODE_LOGS and VCRYPT_ALERT tables, respectively. They join to each other via the REQUEST_ID field, and they each join to the geolocation data via the VCRYPT_IP_LOCATION_MAP table via the BASE_IP_ADDR field.

### 25.8.5.1  Type Code Lookups

The session table and the alert table have several type code fields that may be translated into readable text by following the instructions to look up the user defined enums by name. The following tables will list the type code fields and the name of the user defined enum.

*Table 25–1  VCRYPT_TRACKER_USERNODE_LOGS*

| Field Name | User Defined Enum Name |
| --- | --- |
| AUTH_STATUS | auth.status.enum |
| AUTH_CLIENT_TYPE_CODE | auth.client.type.enum |

*Table 25–2    VCRYPT_ALERT*

| Field Name | User Defined Enum Name |
|---|---|
| ALERT_LEVEL | alert.level.enum |
| ALERT_TYPE | alert.type.enum |
| ALERT_STATUS | alert.status.enum |
| RUNTIME_TYPE | profile.type.enum |

## 25.8.6  Example

This report will show a list of sessions, with user id, login id, auth status, and location. To start with, you will need to create two date parameters, fromDate and toDate. The query will look like this:

```
SELECT s.request_id, s.user_id, s.user_login_id, auth.label, country.country_name,
state.state_name,
city.city_name
FROM vcrypt_tracker_usernode_logs s
      INNER JOIN vcrypt_ip_location_map loc ON s.base_ip_addr = loc.base_ip_addr
      INNER JOIN vcrypt_country country ON loc.country_id = country.country_id
      INNER JOIN vcrypt_state loc ON loc.state_id = country.state_id
      INNER JOIN vcrypt_city city ON loc.city_id = city.city_id
      LEFT OUTER JOIN (
              SELECT enumElement.num_value, enumElement.label
              FROM v_b_enum enum
                    INNER JOIN v_b_enum_elmnt enumElement ON on enum.enum_id =
enum_element.enum_id
              WHERE enum.prop_name = 'auth.status.enum') auth
              ON s.auth_status = auth.num_value
WHERE (:fromDate IS NULL OR s.create_time >= :fromDate)
      AND (:toDate IS NULL OR s.create_time <= :toDate)
ORDER BY s.create_time DESC
```

## 25.8.7  Adding Layouts to the Report Definition

BI Publisher offers several options for designing templates for your reports. Refer to the *Oracle Business Intelligence Publisher Report Designer's Guide* for instructions.

# 25.9  Building OAAM Transactions Reports

This section explains how you can build transaction reports. It contains the following topics:

- Get Entities and Transactions Information
- Discover Entity Data Mapping Information
- Discover Transaction Data Mapping Information
- Build Reports

## 25.9.1  Get Entities and Transactions Information

To get the Transaction Definition key and Entity Definition keys, follow these steps:

1.  Log into OAAM Admin application and go to Transactions menu and search for the transaction definitions you are interested in.

2. Go to the **General** tab and note down the **Definition Key** of the transaction. This is the "Transaction Definition Key" of the transaction.

3. Go to the **Entities** tab of the transaction and note down distinct list **Entity Name**.

4. Choose the **Entities** menu option to search for Entities and note the **Key** of each of those entities. That is the "Entity Definition Key" of the entities.

## 25.9.2 Discover Entity Data Mapping Information

To discover entity data mapping information that you will need to create your report, follow the procedures in this section.

### 25.9.2.1 Information about Data Types

For your reference, number data types are listed in the following table.

*Table 25–3 Information about Data Types*

| Data Type | Description |
| --- | --- |
| 1 | Represents String data |
| 2 | Represents Numeric data. Data stored is equal to (Original value * 1000). |
| 3 | Date type data. Store the data in "'YYYY-MM-DD HH24:MI:SS TZH:TZM" format and also retrieve it using same format. |
| 4 | Boolean data. Stored as strings. "True" represents TRUE and "False" represents FALSE |

### 25.9.2.2 Discover Entity Data Details Like Data Type, Row and Column Mappings

To get the entity data details that you will need to construct your report, follow these steps:

1. Get the Entity Definition Key by looking at the entity definition using the OAAM Admin Console.

2. Get details of how entity data is mapped using the SQL Query:

```
SELECT label,
  data_row,
  data_col,
  data_type
FROM vt_data_def_elem
WHERE status =1
AND data_def_id =
  (SELECT data_def_id
  FROM vt_data_def_map
  WHERE relation_type   ='data'
  AND parent_obj_type   =3
  AND parent_object_id IN
    (SELECT entity_def_id
    FROM vt_entity_def
    WHERE entity_def_key=<Entity Definition Key>
    AND status =1
    )
  )
ORDER BY data_row ASC,
  data_col ASC;
```

### 25.9.2.3 Build Entity Data SQL Queries and Views

The above SQL query gives a list of data fields of the entity with data type and row, column position. Using that information, build a SQL query based on the following information that represents data of the given entity. It is also recommended to create/build a view based on this SQL query that represents data of the given entity.

> **Note:** EntityRowN represents an entity data row. If your entity has 3 distinct data_row values from the above query then you would have 3 EntityRows, name the aliases as EntityRow1, EntityRow2, and so on, and similarly take care of the corresponding joins as shown below.

```
SELECT ent.ENTITY_ID,
    ent.EXT_ENTITY_ID,
    ent.ENTITYNAME,
    ent.ENTITY_KEY,
    ent.ENTITY_TYPE,
    EntityRowN<row>.DATA<col> <column_name>,
    (EntityRowN<row>.NUM_DATA<col>/ 1000.0) <numeric_column_name>,
    to_timestamp_tz(EntityRowN<row>.DATA<col>, 'YYYY-MM-DD HH24:MI:SS TZH:TZM')
<date_column_name>,
    ent.CREATE_TIME,
    ent.UPDATE_TIME,
    ent.EXPIRY_TIME,
    ent.RENEW_TIME
  FROM
    VT_ENTITY_DEF entDef,
    VT_ENTITY_ONE ent
    LEFT OUTER JOIN VT_ENTITY_ONE_PROFILE EntityRowN
  ON (EntityRowN.ENTITY_ID    = ent.ENTITY_ID
  AND EntityRowN.ROW_ORDER    = <row>
  AND EntityRowN.EXPIRE_TIME IS NULL)
    LEFT OUTER JOIN VT_ENTITY_ONE_PROFILE EntityRowN+1
  ON (EntityRowN+1.ENTITY_ID    = ent.ENTITY_ID
  AND EntityRowN+1.ROW_ORDER    = <row+1>
AND row1.EXPIRE_TIME IS NULL)
  WHERE
ent.ENTITY_DEF_ID      = entDef.ENTITY_DEF_ID and
entDef.ENTITY_DEF_KEY=<Entity Definition Key>
```

## 25.9.3 Discover Transaction Data Mapping Information

To discover transaction data mapping information that you will need to create your report, follow the procedures in this section.

### 25.9.3.1 Discover Transaction data details like Data Type, Row and Column mappings

To get entity data details you will need to construct your report, follow these steps:

1. Get list of transaction to entity definition mapping Ids using the following SQL:

```
SELECT map_id
FROM
vt_trx_ent_defs_map,
   vt_trx_def
WHERE
vt_trx_ent_defs_map.trx_def_id = vt_trx_def.trx_def_id
AND vt_trx_def.trx_def_key  =<Transaction Definition Key>
```

2. Use the following SQL query to get details of all transaction data fields, their data type and their row, column mapping:

```
SELECT label,
   data_row,
   data_col,
   data_type
FROM vt_data_def_elem
WHERE status    =1
AND data_def_id =
   (SELECT data_def_id
   FROM vt_data_def_map
   WHERE relation_type  ='data'
   AND parent_obj_type   =1
   AND parent_object_id IN
     (SELECT trx_def_id
      FROM vt_trx_def
      WHERE trx_def_key='mayo_pat_rec_acc'
      AND status       =1
      )
   )
ORDER BY data_row ASC,
   data_col ASC;
```

### 25.9.3.2 Build Transaction Data SQL Queries and Views

Use the information from the previous section and build a SQL query that represents transaction data based on the following:

Note: It is recommended to build a view based on this Query so that it is easier to build reports

```
SELECT trx.LOG_ID,
    trx.USER_ID,
    trx.REQUEST_ID,
    trx.EXT_TRX_ID,
    trx.TRX_TYPE,
    trx.STATUS,
    trx.SCORE,
    trx.RULE_ACTION,
    trx.TRX_FLAG,
    trx.POST_PROCESS_STATUS,
    trx.POST_PROCESS_RESULT,
    TxnDataRowN<row>.DATA<col> <data_column_name>,
    (TxnDataRowN<row>.NUM_DATA<col>/ 1000.0) <numeric_column_name>,
    to_timestamp_tz(TxnDataRowN<row>.DATA<col>, 'YYYY-MM-DD HH24:MI:SS TZH:TZM')
<date_column_name>,
    (SELECT entTrxMap.MAP_OBJ_ID
    FROM VT_ENT_TRX_MAP entTrxMap
    WHERE entTrxMap.DEF_MAP_ID = <Transaction to Entity Mapping Id of Entity1_
Name>
    AND entTrxMap.TRX_ID      = trx.LOG_ID
    ) <EntityN_Name>,
    (SELECT entTrxMap.MAP_OBJ_ID
    FROM VT_ENT_TRX_MAP entTrxMap
    WHERE entTrxMap.DEF_MAP_ID = <Transaction to Entity Mapping Id of Entity2_
Name>
    AND entTrxMap.TRX_ID      = trx.LOG_ID
    ) <EntityN+1_Name>,
```

```
        trx.CREATE_TIME,
        trx.UPDATE_TIME,
        TRUNC(trx.create_time, 'HH24') created_hour,
        TRUNC(trx.create_time, 'DDD') created_day,
        TRUNC(trx.create_time, 'DAY') created_week,
        TRUNC(trx.create_time, 'MM') created_month,
        TRUNC(trx.create_time, 'YYYY') created_year
    FROM VT_TRX_DEF trxDef,
        VT_TRX_LOGS trx
    LEFT OUTER JOIN VT_TRX_DATA TransactionDataRowN
    ON (TransactionDataRowN.TRX_ID        = trx.LOG_ID
    AND TransactionDataRowN.ROW_ORDER     = <rowN>)
LEFT OUTER JOIN VT_TRX_DATA TransactionDataRowN+1
    ON (TransactionDataRowN+1.TRX_ID        = trx.LOG_ID
    AND TransactionDataRowN+1.ROW_ORDER     = <rowN+1>)
    WHERE trx.TRX_DEF_ID      = trxDef.TRX_DEF_ID  and
trxDef.TRX_DEF_KEY=<Transaction Definition Key>
```

## 25.9.4  Build Reports

Follow the instructions in this section to build reports for entities and transactions.

### 25.9.4.1  Building Entity Data Reports

Use the SQL Queries or Views built using the information mentioned in
Section 25.9.2.3, "Build Entity Data SQL Queries and Views."

### 25.9.4.2  Building Transaction Data Reports

Use the SQL Queries or Views built using the information mentioned in
Section 25.9.3.2, "Build Transaction Data SQL Queries and Views."

### 25.9.4.3  Joining Entity Data Tables and Transaction data tables

You can join the transaction data views you built with entity data view using VT_
ENT_TRX_ MAP.MAP_OBJ_ID which is indicated using the pseudo column
<EntityN_Name>.

# 25.10  Adding Translations for the BI Publisher Catalog and Reports

In release 11g, BI Publisher supports two types of translation:

- Catalog Translation

- Template (or layout) Translation

Catalog translation enables the extraction of translatable strings from all objects
contained in a selected catalog folder into a single translation file; this file can then be
translated and uploaded back to BI Publisher and assigned the appropriate language
code.

Catalog translation extracts not only translatable strings from the report layouts, but
also the user interface strings that are displayed to users, such as catalog object
descriptions, report parameter names, and data display names.

Users viewing the catalog will see the item translations appropriate for the user
interface Language they selected in their My Account preferences. Users will see
report translations appropriate for the Report Locale they selected in their My Account
preferences.

Template translation enables the extraction of the translatable strings from a single RTF-based template (including sub templates and style templates) or a single BI Publisher layout template (.xpt file). Use this option when you only need the final report documents translated. For example, your enterprise requires translated invoices to send to German and Japanese customers.

For information describing the process of downloading and uploading translation files, refer to the "Adding Translations for the BI Publisher Catalog and Reports" of the *Oracle Fusion Middleware Administrator's and Developer's Guide for Oracle Business Intelligence Publisher*.

# 25.11 Use Cases

The following section provides a scenario of how Oracle Adaptive Access Manager's reports are used.

## 25.11.1 Use Case: BIP Reports

You are Marty, a business analyst for Acme Corp. You have been asked to gather some aggregate data on the impact to customers by the Oracle Adaptive Access Manager security system.

Directions: Run the KBA challenge statistics report and rules aggregate breakdown report. Also run the recent logins report, filtering for sessions that resulted in a block. Run all the reports with XLS output so you can share the results with your business unit.

### 25.11.1.1 Description

This use case demonstrates how to use BI Publisher.

### 25.11.1.2 Steps

This use case demonstrates how to use BI Publisher reports.

1. Log in to the BI Publisher as an Analyst.

2. Select OAAM under Shared Folders.

3. Under oaam folder, select oradb.

4. Locate the report to run.

   a. Under the Common folder, click **RecentLogins** to view the RecentLogins report.

   b. Under the KBA folder, click **ChallengeStatistics** to view the Challenge Statistics report.

   c. Under the KBA folder, click **QuestionStatistics** to view the QuestionStatistics report

   d. Under the Security folder, click **RulesBreakdown** to view the RulesBreakdown report.

5. For the RecentLogins report, select **Blocked** in Auth Status as a search criteria.

6. Repeat the following steps for each report.

   a. Click **View**.

   b. In Template menu, select **Excel2000** and click **Export**.

## 25.11.2 Use Case: LoginSummary Report

The LoginSummary displays login aggregate summary for the designated date range.

1. Log in to Oracle BI Publisher using a URL of the form:

   ```
   http://host.domain.com:port/xmlpserver/
   ```

2. On the main page, click **OAAM** under Shared Folders and then **oradb**.

3. Under the Security folder, click LoginSummary to view the **LoginSummary** report.

   The Login Summary Report opens with the default time range of one month.

   The summary graph shows the following:

   - The count of sessions

   - The count of users

   - The count of registrations

   - The count of blocks

4. Save or export the report as desired.

# 26

# Monitoring Performance by Using Fusion Middleware Control

This chapter describes how to monitor Oracle Adaptive Access Manager 11*g* performance and shut down and start Oracle Adaptive Access Manager instances using Fusion Middleware Control.

## 26.1 Displaying Fusion Middleware Control

Fusion Middleware Control organizes a wide variety of performance data and administrative functions into distinct, Web-based home pages. The Fusion Middleware Control home pages make it easy to locate the most important monitoring data functions from a Web browser.

To display Fusion Middleware Control:

1.  Enter the Fusion Middleware Control URL, which includes the name of the host and the administration port number assigned during the installation. The following shows the format of the URL:

    ```
    http://hostname.domain:port/em
    ```

2.  Enter the Oracle Fusion Middleware administrator user name and password and click **Login**.

    The default user name for the administrator user is `weblogic`. This is the account you can use to log in to Fusion Middleware Control for the first time. The password is the one you supplied during the installation of Oracle Fusion Middleware.

    The Fusion Middleware Control Login is shown in Figure 26–1.

*Figure 26–1   Fusion Middleware Control Login*
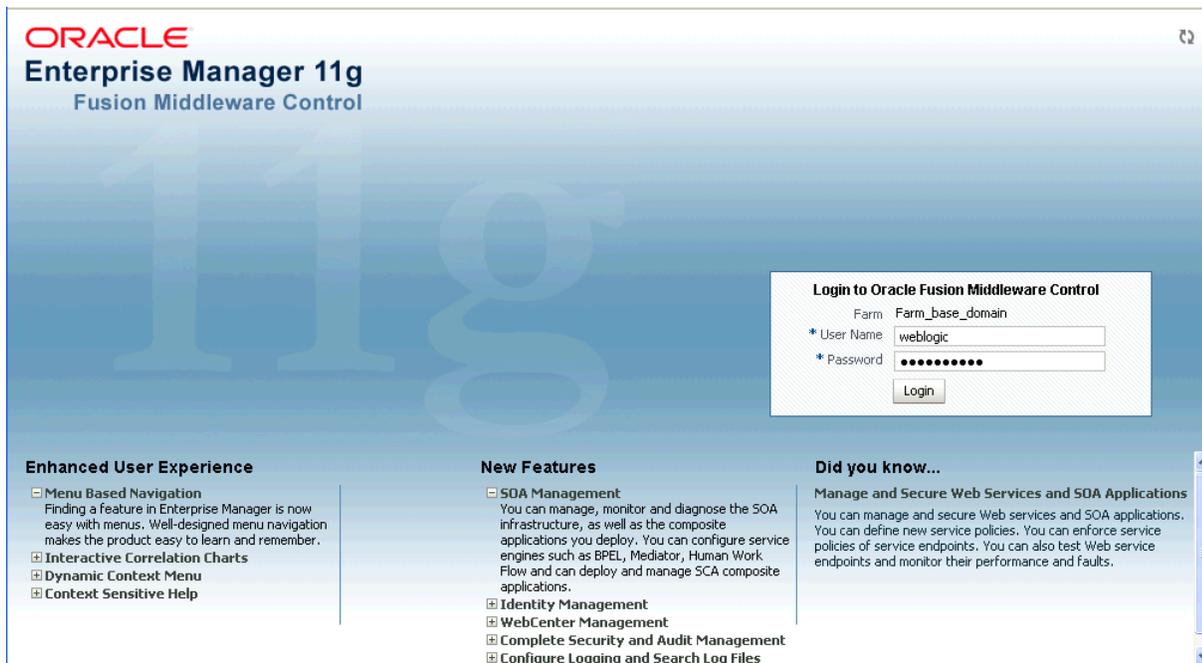


## 26.2  Displaying Base Domain 11*g* Farm Page

When you first log in to Fusion Middleware Control, the Base Domain home page is displayed.

Fusion Middleware Control displays the target navigation pane on the left and the content pane on the right.

The farm home page is shown in

*Figure 26–2   Oracle Adaptive Access Manager Farm Home Page*
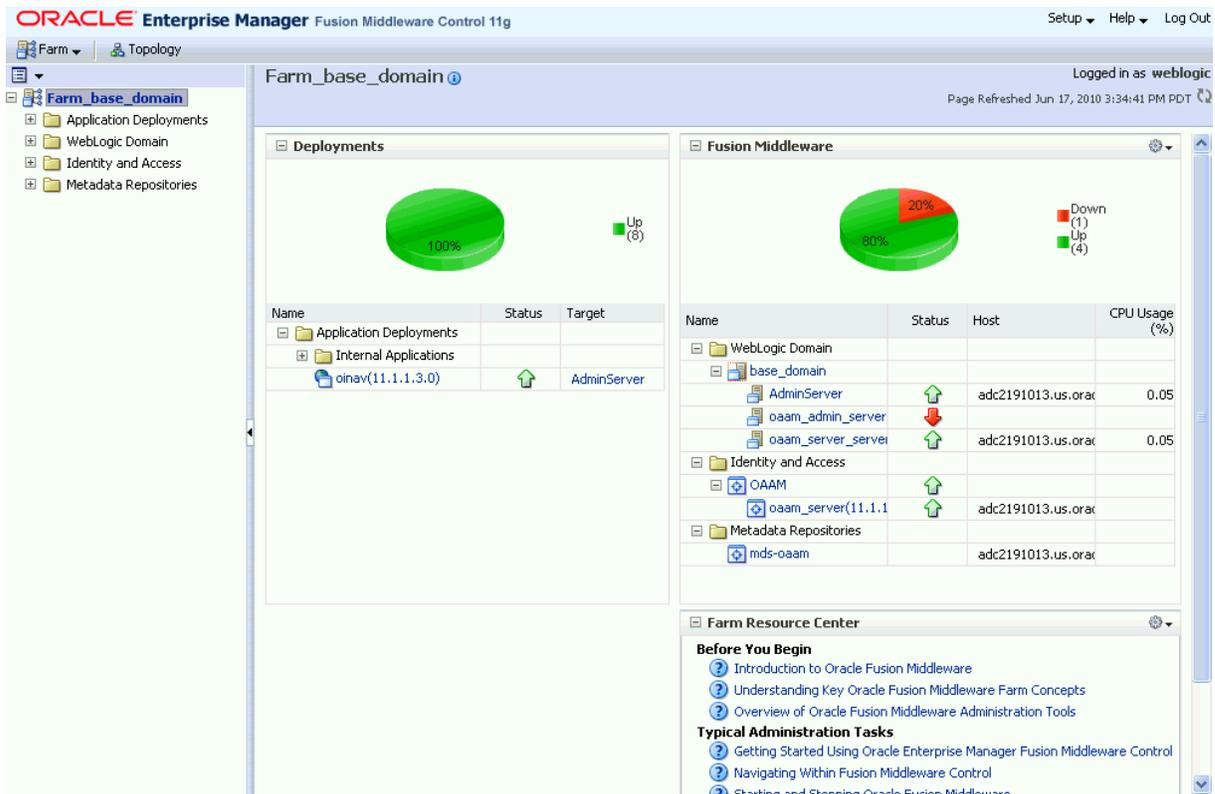


**Content Pane**

The content pane displays the overall status of the Oracle Fusion Middleware environment and links to reference information.

From here, you can view

- The status and target of the internal applications in the deployment.

- The status, host, and CPU usage of the repository and server instances.

- Resource information on concepts and tasks

**Target Navigation Pane**

The target navigation pane lists all of the targets in the farm in a navigation tree.

Oracle Adaptive Access Manager details in Fusion Middleware Control are divided into the following nodes within the navigation pane:

- Application Deployments

- WebLogic Domain

- Identity and Access

- Metadata Repositories

When you select a target, such as a Managed Server or a component, the target's home page is displayed in the content pane and that target's menu is displayed at the top of the page, in the context pane. For example, if you select a Managed Server, the WebLogic Server menu is displayed. You can also view the menu for a target by right-clicking the target in the navigation pane.

**Farm Menu**

Farm Menu in the upper left corner of the target navigation pane provides a list of operations that you can perform on the farm.

*Figure 26–3   Farm Menu*
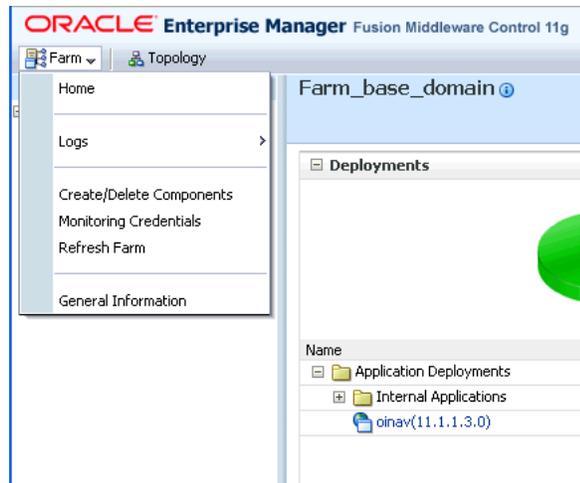


**Dynamic Menu**

Dynamic Target Menu provides a list of operations that you can perform on the currently selected target. The menu that is displayed depends on the target you select. The menu for a specific target contains the same operations as those in the Right-Click Target Menu.

*Figure 26–4   Dynamic Menu*
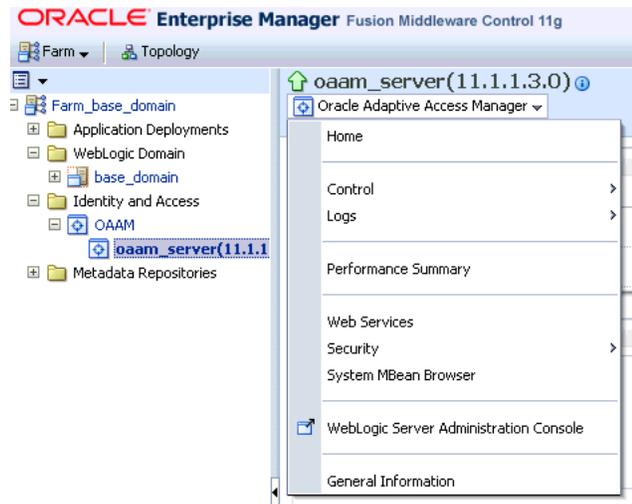


# 26.3  Oracle Adaptive Access Manager Cluster Home Page

To access the Oracle Adaptive Access Manager Cluster Home page:

1.  Log in to Fusion Middleware Control.

2.  Expand the **Identity and Access** node.

3. Click the **OAAM** (cluster) node.

The Oracle Adaptive Access Manager Cluster Home page appears. Use this page to monitor the OAAM cluster.

From the Oracle Access Manager Cluster Home page, you can:

- Monitor the OAAM cluster
- View the status of the OAAM servers that are part of the OAAM cluster
- View details of the database used by Oracle Adaptive Access Manager
- Access general information about the OAAM cluster such as the name, version, Oracle Home, and domain home
- Access the performance summary of the server instances in the cluster

### Monitor the Oracle Adaptive Access Manager cluster

The Performance Overview section of the Oracle Adaptive Access Manager Cluster Home page shows a graphical representation and a table view of the login statistics.

The data shown are for:

- Number of successful logins during the last 5 minute collection interval
- Number of logins failed during the last 5 minute collection interval

In the graphical representation, the x axis shows the time and the y axis shows the number of logins.

The performance overview is also available in tabular format when you click the **Table View** link at the bottom of the graph.

### View the status of the servers that are part of the Oracle Adaptive Access Manager cluster

The Deployment section of the Oracle Adaptive Access Manager Cluster Home page provides information on the statuses of the OAAM server instances.

You can view the following information:

| Fields | Description |
| --- | --- |
| Instance Name | The name of the OAAM server instance. For example: oaam_server. |
| Status | The status of the OAAM server instance:<br><br>■ Green Up Arrow indicates that the instance is running<br><br>■ Red Down Arrow indicates that the instance is not running<br><br>■ Clock indicates that the status information is currently unavailable. |
| Total Logins | The total number of logins attempted since startup. |
| Logins Successful | The total number of successful logins since startup |
| Logins Failed | The total number of failed logins since startup. |

### View details of the database used by Oracle Adaptive Access Manager

To view hostname, port, and Service ID of the data repository, refer to the Data Store section. Oracle Adaptive Access Manager uses the RDBMS database as its data store.

| Fields | Description |
|---|---|
| Hostname | The name of the server where the data store is located. |
| Port | The port on which the Listener is listening for Oracle connections |
| Service ID | The name of the database that Oracle Adaptive Access Manager is using. |

**Access general information about the Oracle Adaptive Access Manager**

From the Oracle Adaptive Access Manager Cluster Home page, you can access general information about the cluster and the datasource.

To view the target name, version, Oracle Home, and Domain home:

1. Click **Oracle Adaptive Access Manager Cluster** at the top of the home page to expand the dynamic menu.

2. Select **General Information**.

**Access the Performance Summary for the Oracle Adaptive Access Manager Cluster**

To see a performance summary for insight into the current performance of the Oracle Adaptive Access Manager cluster:

1. Click **Oracle Adaptive Access Manager Cluster** at the top of the home page to expand the dynamic menu.

2. Click **Performance Summary**.

## 26.4 Oracle Adaptive Access Manager Server Home Page

The Oracle Adaptive Access Manager Server Home page displays a performance overview of the instance.

To access an Oracle Adaptive Access Manager Server Home page:

1. Log in to Fusion Middleware Control.

2. Expand the **Identity and Access** node.

3. Expand the **OAAM** (cluster) node.

4. Click an OAAM server node.

The Oracle Adaptive Access Manager Server Home page appears. From this page, you can:

- View statistic summary for the OAAM server instance

- View performance overview (graphical representation and table)

- Access a List of Operations to perform

**View statistic summary for the Oracle Adaptive Access Manager server instance**

The OAAM Server Home Page displays a Performance Overview with key metrics.

From this page, you can view a statistic summary for the OAAM Server instance that was selected.

| Metric | Description |
|---|---|
| Logins - Logins Successful | Total number of successful logins since startup. |
| Logins - Logins Failed | Total number of login attempts that failed since startup. |
| Checkpoint - Average Processing Time | Average time (in ms) for all the policies in a checkpoint to process since startup. |
| Checkpoint - Number of Checkpoints Processed | Total number of checkpoints processed since startup. |
| Policies - Average Policy Processing Time | Average time (in ms) to process a policy |
| Policies - Number of Polices Processed | Total number of policies processed since startup |

**View performance overview of the Oracle Adaptive Access Manager server instance**

The Performance Overview section of the OAAM Server Home page provides a graphic representations of logins to the OAAM server instance. You can also open a table view of logins from this section.

- Graphical

  The x axis shows the time.

  The y axis shows the number of logins, checkpoints, or policies processed.

- Table

  Click **Table View** to show the Performance Overview in tabular format.

**Access the list of operations to perform on the Oracle Adaptive Access Manager server instance**

The Oracle Adaptive Access Manager menu, which is available when you click Oracle Adaptive Access Manager at the top of the page, provides a list of server instance-related operations. This menu contains the same operations as those in the context menu.

| Menu Item | Operation |
|---|---|
| Home | Allows you to view the instance home page |
| Control | Allows you to start up and shut down the server instance |
| | From the menu, click **Control** and select **Startup** or **Shutdown**. |
| Logs | Allows you to view server logs and configure logging |
| | From the menu, click **Logs** and select **View Log Messages** or **Log Configurations**. |

| Menu Item | Operation |
|---|---|
| Performance Summary | Allows you to view a performance summary<br><br>From the menu, click **Performance Summary**.<br><br>The categories for the summary metrics are:<br>■ CheckPoint Execution Summary<br>■ Login Metrics Summary<br>■ Policy Execution Summary<br>■ Rule Execution Summary<br>■ Rule Processing Summary<br>■ Update Authorization Status Summary<br>■ Update Log Summary<br>■ Web Module Metrics |
| Web Services | Allows you to view web services<br><br>From the menu, click **Web Services**. |
| Security | Allows you to view OAAM Server application policies and roles<br><br>From the menu, click **Security** and select **Application Policies** or **Application Roles**. |
| System MBean Browser | Allows you to access the System MBean Browser<br><br>From the menu, click **System MBean Browser**. |
| WebLogic Server Administration Console | Allows you to access the WebLogic Server Administration Console<br><br>From the menu, click **WebLogic Server Administration Console**. |
| General Information | Allows you to view general information about the server instance<br><br>From the menu, click **General Information**. |

# 27

# Monitor and Audit of Events

This chapter contains the following sections:

- Monitoring Information Sent to Dynamic Monitoring System
- Audit Information Sent to Audit System

## 27.1 Monitoring Information Sent to Dynamic Monitoring System

Oracle Dynamic Monitoring Service (DMS) enables application developers, support analysts, system administrators, and others to measure application-specific performance information.

DMS Instrumentation to Oracle Adaptive Access Manager enables you to collect and analyze performance information. DMS is notified when events occur, when important intervals begin and end, or when pre-computed values change their state. At run time, DMS stores metrics in memory and enables you to save or view the metrics in Fusion Middleware Control.

The following Oracle Adaptive Access Manager information is sent to Dynamic Monitoring System (DMS):

### 27.1.1 Login Information (Counts Only)

Login Information (Counts only) that is sent are:

*Table 27–1    Log In Information*

| Description | DMS Noun Path | DMS Noun Type/Group |
| --- | --- | --- |
| Login Count - Total | /OAMS/OAAM/LoginCount_Total | OAMS.OAAM_Counters |
| Login Count - Success | /OAMS/OAAM/LoginCount_Success | OAMS.OAAM_Counters |
| Login Count - Failed | /OAMS/OAAM/LoginCount_Failed | OAMS.OAAM_Counters |
| Login Count - Blocked | /OAMS/OAAM/LoginCount_Blocked | OAMS.OAAM_Counters |
| Login Count - Challenged | /OAMS/OAAM/LoginCount_Challenged | OAMS.OAAM_Counters |

### 27.1.2 Rules Engine Execution Information (Count and Time Taken to Execute)

The rules engine execution information (count and time taken to execute) is shown in Table 27–2.

**Table 27–2 Rules Engine Execution**

| Description | DMS Noun Path | DMS Noun Type/Group |
|---|---|---|
| Rules Execution | /OAMS/OAAM/Rules_Execution | OAMS.OAAM |
| Policies Execution | /OAMS/OAAM/Policies_Execution | OAMS.OAAM |
| Checkpoints Execution | /OAMS/OAAM/Checkpoints_Execution | OAMS.OAAM |

### 27.1.3 APIs Execution Information (Count and Time Taken to Execute)

The APIs execution information (count and time taken to execute) is shown in Table 27–3

**Table 27–3 API Execution**

| Description | DMS Noun Path | DMS Noun Type/Group |
|---|---|---|
| API Call updateLog | /OAMS/OAAM/API/Tracker/UpdateLog | OAMS.OAAM |
| API Call updateAuthStatus | /OAMS/OAAM/API/Tracker/UpdateAuthStatus | OAMS.OAAM |
| API Call processRules | /OAMS/OAAM/API/RulesEngine/ProcessRules | OAMS.OAAM |

## 27.2 Audit Information Sent to Audit System

Oracle Fusion Middleware Audit Framework is a new service in 11*g* Release 1 (11.1.1), designed to provide a centralized audit framework for the middleware family of products. Oracle Fusion Middleware Audit Framework is integrated with Oracle Business Intelligence Publisher for out-of-the box reports.

Oracle Adaptive Access Manager 11*g* logs the following events using the Oracle Audit Framework:

### 27.2.1 Customer Care Events

Customer Care Events are shown in Table 27–4.

**Table 27–4 Customer Care Events**

| Event Name | Event Data | Notes |
|---|---|---|
| Create CSR Case | CaseId, UserGroupName, UserId, CaseSeverity, Description | |
| Update Cases | CaseId, CaseSeverity, CaseStatus, CaseDisposition, CaseExpirationDurationInHrs, ActionNotes, CaseActionResult | |
| Change Status | CaseId, CaseStatus, CaseDisposition, ActionNotes, CaseActionResult | |
| Perform Case Action | CaseId, CaseActionEnum, CaseSubActionEnum, ActionNotes, CaseActionResult | |
| Get Challenge Question | CaseId, ActionNotes, CaseChallengeQuestion | |
| Check Challenge Question Response | CaseId, ActionNotes, CaseChallengeQuestion, CaseChallengeQuestionResult | |

## 27.2.2  Policy Management Events

Policy Management Events are listed in Table 27–5.

**Table 27–5    Policy Management Events**

| Event Name | Event Data | Notes |
|---|---|---|
| Create Policy | PolicyId, PolicyName, PolicyDetails | |
| Copy Policy | SourcePolicyId, PolicyName, PolicyDetails | |
| Update Policy | PolicyId, PolicyName, PolicyDetails | |
| Delete Policy | PolicyIds | |
| Add Override | PolicyId, PolicyOverrideRowId, PolicyOverrideDetails | |
| Update Overrides | PolicyId, PolicyOverrideIds, PolicyOverrideDetails | |
| Delete Overrides | PolicyId,PolicyOverrideIds | |
| Link Policy To Group | PolicyId,GroupId, ActionNotes | |
| Unlink Policy from Groups | PolicyId,GroupIds | |
| Create Rule | PolicyId, RuleId, RuleName, RuleDetails | |
| Add Conditions to Rule | PolicyRuleMapId, RuleConditionIds | |
| Update Rule in Policy | PolicyId, RuleId, RuleName, RuleDetails | |
| Copy Rule to Policy | PolicyId,PolicyRuleMapDetails | |
| Delete Rules from Policy | PolicyRuleMapIds | |
| Update Rules Order in Policy | PolicyRuleMapId, RuleConditionMapIds | |
| Update Rule Parameter values | PolicyRuleMapId, RuleConditionMapId, RuleParamValueDetails | |

## 27.2.3  KBA Questions Events

KBA Questions Events are listed in Table 27–6.

**Table 27–6    KBA Questions Events**

| Event Name | Event Data | Notes |
|---|---|---|
| Create KBA Category | KBACategoryId, KBACategoryName, KBACategoryDetails | |
| Update KBA Category | KBACategoryId, KBACategoryName, KBACategoryDetails | |
| Delete KBA Categories | KBACategoryIds | |
| Create KBA Question | KBAQuestionId, KBAQuestion, KBAQuestionDetails | |
| Update KBA Question | KBAQuestionId, KBAQuestion, KBAQuestionDetails | |
| Delete KBA Questions | KBAQuestionIds | |
| Create KBA Validation | KBAValidationId, KBAValidationName, KBAValidationDetails | |

*Table 27–6  (Cont.) KBA Questions Events*

| Event Name | Event Data | Notes |
|---|---|---|
| Update KBA Validation | KBAValidationId, KBAValidationName, KBAValidationDetails | |
| Delete KBA Validation | KBAValidationIds | |
| Add KBA Validation to Global | KBAValidationId | |
| Delete KBA Validation from Global | KBAValidationId | |
| Update KBA Answer Logic | KBAAnswerLogicDetails | |
| Update KBA Registration Logic | KBARegistrationLogicDetails | |

## 27.2.4 Group/List Management Events

Group/List Management Events are listed in Table 27–7.

*Table 27–7  Group/List Management Events*

| Event Name | Event Data | Notes |
|---|---|---|
| Add Group | GroupId, GroupName, GroupDetails | |
| Update Group | GroupId, GroupName, GroupDetails | |
| Delete Groups | GroupIds | |
| Add Group Elements | GroupId, GroupElementsDetails | |
| Update Group Element | GroupId, GroupElementId, GroupElementValue | |
| Delete Group Elements | GroupId, GroupElementIds | |
| Delete all Group Elements | GroupId | |

# Part X

## Deployment Management

This part of the book contains information about managing deployment in Oracle
Adaptive Access Manager.

# 28

# Using the Properties Editor

Oracle Adaptive Access Manager provides properties out-of-the-box and a Properties Editor that enables you to create new database properties according to your requirement, modify existing database and file properties, and create and edit enumerations.

Note: not all roles have permissions to access the Properties Editor.

This chapter focuses on properties management using OAAM Admin. It includes the following topics:

- Navigating to the Properties Search Page
- Searching for a Property
- Viewing the Value of a Property
- Viewing Enumerations
- Creating a New Database Type Property
- Editing the Values for Database and File Type Properties
- Deleting Database Type Properties
- Exporting Database and File Type Properties
- Importing Database Type Properties

## 28.1 Navigating to the Properties Search Page

The Properties Search page is the starting place for managing your property definitions.

To open the Properties Search page:

1. In the Navigation tree, double-click **Properties** under **Environment**.

   Alternatively, you can:

   - Right-click **Properties** in the Navigation tree and select **List Properties** from the context menu.

   - Select **Properties** in the Navigation tree and then choose **List Properties** from the **Actions** menu.

   - Click the **List Properties** button in the Navigation tree toolbar.

   The Properties Search page is displayed.

2. Click **Search** to view a list of properties in the system.

## 28.2 Searching for a Property

On the Properties Search page you can view a list of all properties in the system and search for a property based on the name, load type, and value.

*Figure 28–1  Properties Page*
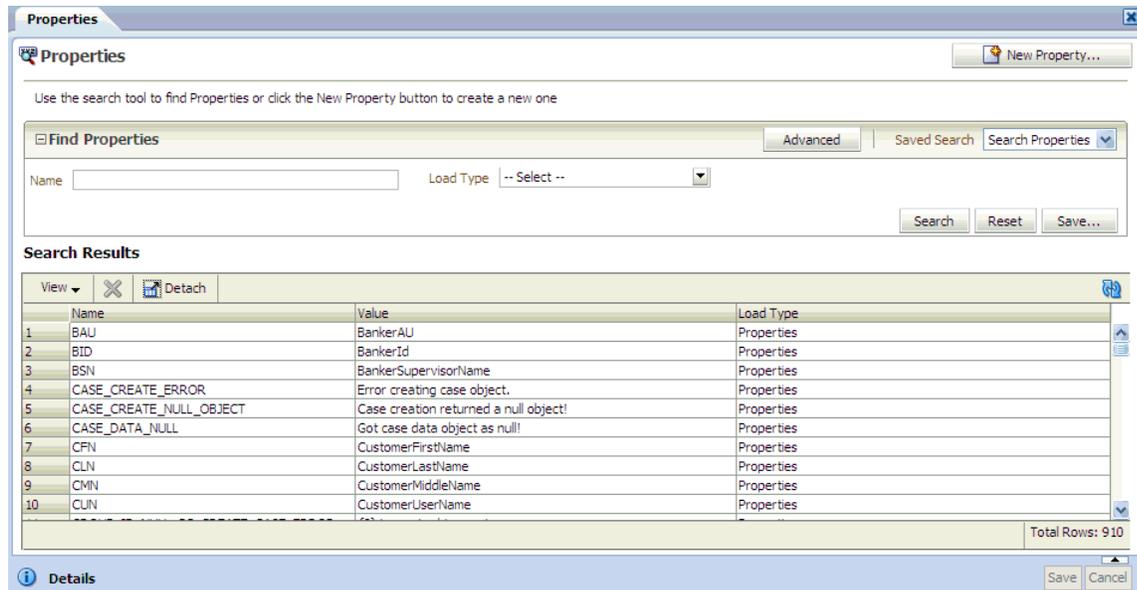


To view a list of the properties present in the system, click **Search**. All available properties are displayed in the Results table.

To search for a property:

1.  Specify the criteria in the search fields in the Properties Search page to locate the property.

    The search filter criteria are described in .

*Table 28–1     Search Filter Criteria*

| Field | Description |
| --- | --- |
| Name | The property name. |
| Load Type | The property's load type. If the property is available in the database, its load type is database; if the property is in a property file, its load type is properties, and if the property is a system property, its load type is systems. By default the load type is set to "all." |
| Value | The value for the property. |

2.  Click **Search**.

    If you want to reset the search parameters to the default setting, use the **Reset** button.

    The Results Table displays a summary of the properties that match the criteria specified.

    By default, properties are sorted on Property Name, but you can sort properties on the Load Type.

## 28.3 Viewing the Value of a Property

To view the value of a property, select the property in the Results table. The name, load type, and value for the property is displayed in the bottom panel.

## 28.4 Viewing Enumerations

Enumerations can be viewed and edited using the Properties Editor.

For the enumerations to be listed in the Properties Editor, you must set the following property to false:

```
bharosa.config.ui.list.filter.enum=false
```

## 28.5 Creating a New Database Type Property

To create a new database type property:

1. From the Properties Search page, click the **New Property** button or **Create new Property** icon.

   A New Property dialog is displayed.

2. In the New Property dialog, type in the property name and value.

   An error message appears for the following:

   - Duplicate name

   - Special characters

   - Blank value

   - Name or value that is more than the maximum length of 4000 ASCII characters or 1333 UTF-8 characters

   The property name cannot be edited after the property has been created.

3. Click **Save**.

All properties created using the properties editor can be of the "Database" type only. They are created in the server database.

A system and file type properties cannot be created from the user interface.

If you do not want to create the new property, click **Cancel** instead of **Save**.

## 28.6 Editing the Values for Database and File Type Properties

You can easily edit the values for database and file type properties and save them.

System properties are read only and cannot be edited.

To edit a database or file type property, follow these steps:

1. In the Results table, select the property.

   The name, load type, and value is shown in the details panel.

   If multiple properties are selected, details for the last selected property are shown in the details panel.

2. In the details panel, edit the value of the property.

   Name and Type are read-only in the details panel.

3. Click **Save**.

   The modified property detail are saved successfully.

   When a file load type property is edited, it changes to a database type property. The existing file type property will no longer be shown in the Results table.

   If you do not want to save the modified property, click **Cancel** instead of **Save** to revert the changes to the original value.

## 28.7 Deleting Database Type Properties

System and file properties are not allowed to be deleted.

To delete a database type property or properties:

1. In the Results table, select the properties.

   A confirmation dialog appears.

2. Click the **Delete** button. The selected properties are deleted successfully.

If you delete a database type property that had been changed from a file type property, the selected property is deleted and the old file type property is restored.

## 28.8 Exporting Database and File Type Properties

To export file properties, follow these steps:

> **Note:** System properties will not be exported. Only file and database type properties will be exported.

1. In the Navigation tree, open **Properties** under Environment.

   The Properties Search page is displayed.

2. Click **Search** to view a list of properties in the system.

3. Select the properties you want to export.

4. Select **Export Selected** from the Actions menu.

   An Export Properties dialog appears with options to select the export type and provide a name.

5. Enter a name for your ZIP file.

6. Choose Java Properties or XML Properties as the Export Type.

7. Click **Export**.

   If you do not want to export the files, click **Cancel** instead of **Save**.

8. Click **Save** and then **OK**.

   A ZIP file for the selected properties in XML or Java format is exported.

## 28.9 Importing Database Type Properties

To import database type properties, follow these steps:

1. In the Navigation tree, open **Properties** under Environment.

The Properties Search page is displayed.

2. Click the **Import Properties** button.

   An Import Properties dialog appears.

3. In the Import Groups dialog box, type the path and name of the file; or use the **Browse** (...) button to locate the ZIP file that contains the properties, and then select the file.

4. Click **Open** and then click **OK**.

   Updates are saved to the database. Updates occur only if the value of the property changed.

5. Click **OK**.

   If you try to import properties in an invalid format, an error will be displayed.

# Part XI

## Command-Line Interface

This part describes how to set up and use Oracle Adaptive Access Manager's command-line interface.

# 29

# Oracle Adaptive Access Manager Command-Line Interface Scripts

This chapter provides information on the Command-Line Interface (CLI).

It contains the following sections:

- CLI Overview
- Setting Up the CLI Environment
- Using CLI
- Importing IP Location Data

## 29.1 CLI Overview

The Oracle Adaptive Access Manager Command-Line Interface (CLI) scripts enable users to perform various tasks instead of using OAAM Admin.

You can use Oracle Adaptive Access Manager CLI scripts for the following:

- Import or export objects like policies, groups, conditions, and other modules without using the graphical user interface.
- Load location data into the Oracle Adaptive Access Manager database

## 29.2 Setting Up the CLI Environment

Setting up the CLI environment involves the following tasks:

1. Set up the CLI work folder
2. Set up the Credential Store Framework (CSF) configuration
3. Set up the Oracle Adaptive Access Manager database credentials

### 29.2.1 Set up the CLI Work Folder

Copy the CLI folder *$IDM_ORACLE_HOME*/oaam/cli/oaam_cli to a working directory, for example, "oaam_cli".

> **Note:** This task is required since it is not recommended to edit or change any files that are inside the IDM_ORACLE_HOME folder (the folder where you installed the IDM software).

**In Unix:**

Execute the following command:

```
cp -r <IDM_ORACLE_HOME>/oaam/cli ~/work/oaam_cli
```

**In Windows**

Execute the following command:

```
xcopy/s   <IDM_ORACLE_HOME>\oaam\cli   c:\work\oaam_cli
```

Select D=directory when it prompts so that entire folder can be copied.

## 29.2.2  Set Up the Credential Store Framework (CSF)

Choose one of the following mechanisms to access the Oracle Adaptive Access Manager Encryption keys stored in the Credential Store Framework (CSF):

- CSF without Mbeans
- CSF with MBeans

### 29.2.2.1  Use CSF without MBeans

Important notes about this approach are listed as follows:

- This method requires that you run the Oracle Adaptive Access Manager command-line utility scripts on the same computer as the WebLogic Server.
- This method does not require you to specify the WebLogic Administrator and password.
- This method is not recommended if Oracle Adaptive Access Manager is deployed in a clustered environment

To use this mechanism:

1. Go to the work folder where you copied the cli folder. Open the file, conf/bharosa_properties/oaam_cli.properties in a text editor and set the following properties:

| Property Name | Notes about Property Value |
|---|---|
| oaam.csf.useMBeans | false |
| oaam.jps.config.filepath | Set the absolute path of jps-config-jse.xml. Usually, it resides in *$DOMAIN_HOME*/config/fmwconfig folder |

2. In a text editor set the following properties related to the Oracle Adaptive Access Manager database:

| Property Name | Notes about Property Values |
|---|---|
| oaam.db.url | Specify valid JDBC URL of the Oracle Adaptive Access Manager database. Make sure there are no typos. |
| oaam.db.additional.properties.file | Leave this as blank if there are no additional toplink properties.<br><br>Otherwise specify the name of the properties file that has additional toplink properties. Make sure the file is in the same folder as oaam_cli.properties |

| Property Name | Notes about Property Values |
|---|---|
| oaam.db.driver | `oracle.jdbc.driver.OracleDriver` (Change this value only if the Oracle Adaptive Access Manager schema is in non-oracle database) |
| oaam.db.min.read-connections | 1 (Do not change this value unless required) |
| oaam.db.max.read-connections | 25 (Do not change this value unless required) |
| oaam.db.min.write-connections | 1 (Do not change this value unless required) |
| oaam.db.max.write-connections | 25 (Do not change this value unless required) |

### 29.2.2.2 Use CSF with MBeans

Important notes about this approach:

- This method is recommended if Oracle Adaptive Access Manager is deployed in a clustered environment.

- This method permits you to remotely connect to the Oracle Adaptive Access Manager WebLogic Server.

- This method requires you to specify the Oracle Adaptive Access Manager WebLogic Admin user and password.

To configure the Oracle Adaptive Access Manager Database details with CSF with MBeans, follow these steps:

1. Go to the work folder where you copied the `cli` folder. Open the file `conf/bharosa_properties/oaam_cli.properties` in a text editor and set the following properties:

| Property Name | Notes about Property Value |
|---|---|
| oaam.csf.useMBeans | true (Keep it as true) |
| oaam.adminserver.hostname | <Host name where WebLogic Admin Server runs> |
| oaam.adminserver.port | <Port number of WebLogic Admin Server. Usually it is 7001> |
| oaam.adminserver.username | <User name of the WebLogic admin user. Usually it is WebLogic> |
| oaam.adminserver.password | <Password of the WebLogic admin user> |

2. Open the file, `conf/bharosa_properties/oaam_cli.properties` in a text editor and set the following properties related to the Oracle Adaptive Access Manager database:

| Property Name | Notes about Value |
|---|---|
| oaam.db.url | Specify valid JDBC URL of the Oracle Adaptive Access Manager database. Make sure there are no typos. |
| oaam.db.additional.properties.file | Leave this as blank if there are no additional toplink properties. Otherwise specify the name of the properties file that has additional toplink properties. Make sure the file is in the same folder as `oaam_cli.properties` |
| oaam.db.driver | oracle.jdbc.driver.OracleDriver (Change this value only if the Oracle Adaptive Access Manager schema is in non-oracle database) |
| oaam.db.min.read-connections | 1 (Do not change this value unless required) |

| Property Name | Notes about Value |
|---|---|
| oaam.db.max.read-connections | 25 (Do not change this value unless required) |
| oaam.db.min.write-connections | 1 (Do not change this value unless required) |
| oaam.db.max.write-connections | 25 (Do not change this value unless required) |

### 29.2.3 Set the Oracle Adaptive Access Manager Database Credentials in the Credential Store Framework

Refer to Section 2.4.7, "Setting Up Oracle Adaptive Access Manager Database Credentials in the Credential Store Framework" for steps.

> **Note:** If you want to use `persistence.xml` instead of setting the Oracle Adaptive Access Manager database credentials in CSF, go through the following steps. However this approach is not recommended and supported.

1. Go to the work folder where you copied the `cli` folder. Open the file `conf/bharosa_properties/oaam_cli.properties` in a text editor and set the property value of `oaam.db.toplink.useCredentialsFromCSF` to `false`.

2. Update the Oracle Adaptive Access Manager database connection details in the `META-INF/persistence.xml` file by editing the relevant `eclipselink.jdbc` properties, as in the following examples:

```
<property name="eclipselink.jdbc.driver"
value="oracle.jdbc.driver.OracleDriver"/>
<property name="eclipselink.jdbc.url"
value="jdbc:oracle:thin:@<dbhost.mydomain.com>:1521/<SERVICE_NAME>"/>
<property name="eclipselink.jdbc.user" value="<OAAM DB USER>"/>
<property name="eclipselink.jdbc.password" value="< DB Password >"/>
```

## 29.3 Using CLI

The Oracle Adaptive Access Manager CLI is a tool in which you can perform various tasks using the keyboard rather than OAAM Admin.

You can use Oracle Adaptive Access Manager CLI in the following ways:

- import or export objects like policies, groups, conditions, and other modules without using the graphical user interface

- perform import and export between different environments (for example, QA and staging) using a program.

- load location data

Set up the Oracle Adaptive Access Manager CLI environment before you run any of the scripts. For details refer to Section 29.2, "Setting Up the CLI Environment."

### 29.3.1 Obtaining Usage Information for Import or Export

To obtain usage information on Oracle Adaptive Access Manager CLI for import or export:

1. At the command line, change to the Oracle Adaptive Access Manager CLI work folder.

2. Run the `runImportExport.sh` script without any arguments.

```
$ sh runImportExport.sh
```

## 29.3.2 Command-Line Options

This subsection provides details about the command-line options.

To perform an import or export, you enter commands coupled with:

- information for actions like import or export
- information for module like policies, groups, validations, or others
- arguments for whether to export or import different modules
- additional parameters for the import and export features.

### 29.3.2.1 What is the Syntax for Commands?

Use this syntax for the command-line interface (typed in a single line with no line breaks or carriage returns):

sh runImportExport.sh

 |-- action < import | export >

 |    +-- <export>

 |    +    |-- entitycmd < add | delete >

 |    +    |-- exportmode < zip | file >

 |    +    |-- includeelements < true | false >

 |    +    |-- listelemcmd < add | delete | replace >

 |    +    -- outdir < path_to_dest_dir >

 |    +-- <import>

 |          -- batchmode < true | false >

-- module < rules | groups | policy(models) | questions | validations | answerHint | properties | conditions | questionsForTranslation | patterns | entities | transactions | dynamicActions | taskGroups >

    +-- <groups>"

       -- submodule < all | users | alerts | ... >

    +-- <properties>"

       -- name < propertyId >

       -- loadType < database | properties | system >

    +-- <conditions>"

       -- forceUpdate < true | false >

       -- adminUser < username >

       -- adminPassword < password >

### 29.3.2.2 CLI Parameters

The options are described in Section 29.3, "Using CLI.".

*Table 29–1    CLI Parameters*

| Parameters | Description |
| --- | --- |
| entitycmd | Indicates whether the entities for the module being exported would be added to the database or deleted from the database on importing the file. Default is add |
| exportmode | Indicates whether the result of export will be a ZIP file or XML file. Default is ZIP. |
| includeelements | Indicates whether the group elements need to be included in export. Default is true. This is applicable only for export of groups. |
| listelemcmd | Indicates whether the group elements will be added, deleted for replaced in the database when this file is imported. Default is add. This is applicable only for groups export. |
| outdir | The output folder where the resulting files from export will be saved. Default value is current folder. |
| batchmode | Controls the database commits when list items are imported in a batch. When the batch reaches its limit, the objects are inserted into the database. If `batchmode` is equal to true, the database update is also committed. By default, `batchmode` is set to `false`. |
| submodule | Used to specify the type of groups that should be included in export. Default value is all. This is applicable for groups export. |
| loadType | Used to specify the type of properties that need to be exported. If not specified then all type of properties are included. This is applicable for properties export. |

### 29.3.2.3  Supported Modules for Import and Export

The list of supported modules for Oracle Adaptive Access Manager 11*g* is shown in Table 29–2.

*Table 29–2    Support Modules*

| Module | Entity Name |
| --- | --- |
| groups | groups |
| policies | models |
| questions | questions |
| validations | validations |
| answer hint | answerHint |
| properties | properties |
| conditions | conditions |
| questions for translation | questionsForTranslation |
| patterns | patterns |
| entities | entities |
| transactions | transactions |
| configurable actions | dynamicActions |
| scheduler task groups | taskGroups |

The 10*g* policy set and policy modules are not longer valid in 11*g*.

The difference between CLI import/export in 10*g* and 11*g* is that the module `models` and `policies` means the same: `–module policy` is same as `-module models`.

### 29.3.2.4  Import of Files

Examples of import options are as follows:

**Import from a File**

To import from a file, issue the following command:

```
$ sh runImportExport -action import -module properties
exportData\properties\<properties_zip_file>
```

**Import Contents of ZIP file**

To import the contents of a ZIP file, issue the following command:

```
$ sh runImportExport.sh -action import -module <supported_
module> <filename>
```

Here are examples:

To upload challenge questions, issue the following command:

```
$ sh runImportExport.sh -action import -module questions
<filename>
```

To import conditions, issue the following command:

```
$ sh runImportExport.sh -action import -module conditions
<filename>
```

To import policies, run the following command

```
$ sh runImportExport.sh -action import -module models <filename>
```

To import groups, run the following command

```
$ sh runImportExport.sh -action import -module groups <filename>
```

**Import a Groups of Users in an XML File**

To import a group of users in an XML file, issue the following command:

```
$ sh runImportExport.sh -action import -module groups <abc.xml>
```

**Import Multiple Policies from Multiple ZIP Files**

To import multiple policies in multiple XML file, issue the following command:

```
$ sh runImportExport.sh -action import

-module models <ManyModels.zip> <OneModel.zip>
```

**Import Multiple Questions from Multiple ZIP Files**

To import multiple questions from multiple ZIP files, issue the command:

```
$ sh runImportExport.sh -action import

-module questions <ManyQuestions.zip> <OneQuestions.zip>
```

**Import Multiple Validations from Multiple ZIP Files**

To import multiple validations from multiple ZIP files, issue the command:

```
$ sh runImportExport.sh -action import

-module validations <ManyValidations.zip> <OneValidations.zip>
```

> **Note:** You may note that inapplicable options will be silently ignored (for example, the `outdir` option used for import) and options with lower precedence will be overridden (for example, `listelemcmd` is irrelevant when `includeelements` is equal to `false`).

### 29.3.2.5  Export of Files

Here are examples of export options:

#### Export Properties

To export all the properties irrespective of `loadtype`, issue the following command:

```
$ sh runImportExport.sh -action export -module properties
```

To export all the properties of any particular `loadtype`, issue the following command:

```
$ sh runImportExport.sh -action export -module properties
-loadtype < database | properties | system>
```

For example, to export all the properties of database `loadtype`, issue the following command:

```
$ sh runImportExport.sh -action export -module properties
-loadtype database
```

To export any single property, issue the following command:

```
$ sh runImportExport.sh -action export -module properties -name
<propertyname>
```

#### Export All

When performing an export, if no entity names are specified, all the entities of that particular module (and submodule) are exported. Thus, specifying names is not necessary for export.

To export all entities of a particular module, issue the following command:

```
$ sh runImportExport.sh -action export -module <module entity_
name>
```

#### Export all Policies

To export all policies, issue the following command:

```
$ sh runImportExport.sh -action export -module models
```

#### Export all User Groups

To export groups, issue the following command:

```
$ sh runImportExport.sh -action export -module groups -submodule
users
```

#### Export All Questions

To export questions, issue the following command:

```
$ sh runImportExport.sh -action export -module questions
```

CLI exports all the related categories, validations, and locale information to make these questions complete.

**Export All Validations:**

To export all validations, issue the following command:

```
$ sh runImportExport.sh -action export -module validations
```

**Export Conditions**

To export conditions, issue the following command:

```
$ sh runImportExport -action export -module conditions
```

**Export Condition with Delete Script**

To export conditions with a delete script, issue the following command:

```
$ sh runImportExport -action export -module conditions
-entitycmd delete
```

**Export Specific Groups, Grp1 and Grp2, without Elements for Delete**

To export specific groups without elements, issue the following command:

```
$ sh runImportExport.sh -action export
```

```
-module groups -includeelements false -entitycmd delete Grp1
Grp2
```

`entitycmd` indicates whether the entities for the module being exported would be added to the database or deleted from the database on importing the file.

In this example, Groups `Grp1` and `Grp2` are deleted from the database when the resulting file from this export command is imported back.

**Export Groups with List Command Replace**

To export groups with list command replace, issue the following command:

```
$ sh runImportExport.sh -action export -module groups
-listelemcmd replace G1 G2
```

The group elements for groups `G1` and `G2` will be replaced by the elements in the ZIP file during the import of the file resulting from this export command. For example, if group `G1` has elements `e1` and `e2` in the database, and the ZIP file has elements `e2` and `e3`, after the execution of the import, group `G1` will have elements `e2` and `e3`. However, if the value of `listelemcmd` had been "`add`," then after the import, `G1` would have elements `e1`, `e2` and `e3`. If the value specified was "`delete`," then after import, group `G1` would have element `e1` only as `e2` would have been deleted.

**Export Policies to DESTDIR, But Do Not Create a ZIP File**

To export policies to DESTDIR, but not create a ZIP file, issue the following command:

```
$ sh runImportExport.sh -action export -outdir DESTDIR
-exportmode file
```

```
-module groups Group1 Group2
```

If `exportmode` is "`file`," then the data is exported as one or more XML files.

> **Note:** The command does not work for modules like policies and questions which have dependent data. A error will occur with the message that a ZIP stream is expected.

### 29.3.2.6 Import Options

The `batchmode` option controls the database commits when list items are imported in a batch. When the batch reaches its limit, the objects are inserted into the database. If `batchmode` is equal to `true`, the database update is also committed. By default, `batchmode` is set to `false`.

```
batchmode {true | false}
```

> **Note:** `batchmode` is not to be used in conjunction with importing other modules. It should be used with Lists only.

Here is an example of `batchmode` usage:

**Import Groups in Batch Mode**

To import groups in batch mode, issue the following command:

```
$ sh runImportExport.sh -action import -module groups -batchmode
true
```

### 29.3.2.7 Importing Multiple Types of Entities in One Transaction

The examples preceding cover only those scenarios where the entities to be processed are of the same type. To be able to process different types of modules together, the command line has been altered to support multiple modules. All entities specified in a command are processed in a single transaction, which allows a related set of entities to be used together to ensure the "all or nothing" approach.

Here are examples of importing modules together:

**Import Various Modules Together**

To import various modules together, issue the following command:

```
$ sh runImportExport.sh -action import

-module groups 5grps.zip

-module models model1.zip
```

> **Note:** The action parameter is not to be repeated, but only the command from the `-module` parameter is repeated as per the different items to be imported. The order of the items supplied in the command line is retained for both, the type of entities, and the files for each entity.

### 29.3.2.8 Multiple Modules and Extra Options (Common vs. Specific)

Support for multiple modules raises many questions:

- What about the extra options?

- How to specify options common to all modules?

- How to specify options specific to a certain module, even though it has been defined as a common option?

The following things can be kept in mind:

- When writing an import or export command, keep in mind that -module is considered as the beginning of a new set of options. Everything that follows -module forms one set of options.

- Everything that is specified before the first -module option is taken as a set of common options, which are applied to each -module.

- If a certain option is specified as a common option and is also specified as a module specific option, the specific value will take precedence.

Examples are:

**Export Everything to "all" Directory, but Policies to "policies" directory**

To export everything to "all" directory, but policies to "policies" directory, issue the following command:

```
$ sh runImportExport.sh -action export -outdir all

-module models -outdir models

-module groups
```

**Export Groups G1 and G2 for Delete Items, and G3 and G4 for Replace Items**

To export groups G1 and G2 for delete items and G3 and G4 for replace items, issue the following command:

```
$ sh runImportExport.sh -action export

-module groups -listelemcmd delete G1 G2

-module groups -listelemcmd replace G3 G4
```

### 29.3.2.9 Transaction Handling

Transaction handling is different from imports and exports.

Import operates strictly in one transaction, except when using batch mode for importing lists. If there is any error in importing any entity for any module, the entire process is rolled back. Thus, no database updates will be committed. You may also note that though import strictly follows one transaction, it does not break down if it encounters invalid items in a list (for example, importing a city with an incorrect state or a country, and so on.) A warning message is logged and the import process continues, ignoring such items.

Export operates on a "best effort" basis. If an export for any entity fails, it continues with the next entity. The reason is that export does not perform any database updates. It only selects information from the database and places it into files.

### 29.3.2.10 Upload Location Database

To use the IP location loader utility, follow the setup instructions in Section 29.4, "Importing IP Location Data."

## 29.3.3 Globalization

For this release, CLI is not globalized.

## 29.4 Importing IP Location Data

This section describes how to import IP location data into the Oracle Adaptive Access Manager database. This data is used by the risk policies framework to determine the risk of fraud associated with a given IP address.

This section contains the following subsections:

- Loading the Location Data to the Oracle Adaptive Access Manager Database
- System Behavior
- Quova/Neustar File Layout
- Oracle Adaptive Access Manager Tables
- Verifying When the Loading was a Success

### 29.4.1 Loading the Location Data to the Oracle Adaptive Access Manager Database

Set up the Oracle Adaptive Access Manager CLI environment before you run any of the scripts. For details refer to Section 29.2, "Setting Up the CLI Environment."

#### 29.4.1.1 Setting Up for SQL Server Database

To load data to Microsoft SQL Server database, `sqljdbc.jar` should be copied to a third party directory. This file can be downloaded for free from Microsoft at `http://www.microsoft.com/downloads/details.aspx?FamilyID=6d48386 9-816a-44cb-9787-a866235efc7c&DisplayLang=en`

#### 29.4.1.2 Setting Up IP Location Loader Properties

1. Change to the `<ORACLE_MW_HOME>/<IAM_HOME>/oaam/cli` directory and make a copy of the sample `bharosa_location.properties` file.

   ```
   cp sample.bharosa_location.properties bharosa_location.properties
   ```

2. Update `bharosa_location.properties` with the location data details as in the following example. The location data should be obtained from one of the supported vendors (`ip2location`, `maxmind`, `Quova/Neustar`).

Note that the properties marked as "Advanced" are not to be changed in general.

*Table 29–3   IP Loader Properties*

| IP Loader Properties | Description |
| --- | --- |
| location.data.provider | quova or ip2location or maxmind |
| location.data.file | /tmp/quova/EDITION_Gold_2008-07-22_v374.dat.gz |
| location.data.ref.file | /tmp/quova/EDITION_Gold_2008-07-22_v374.ref.gz |
| location.data.anonymizer.file | /tmp/quova/anonymizers_2008-07-09.dat.gz |
| location.data.location.file | only if maxmind location data is to be loaded; else leave this property unset/blank |
| location.data.blocks.file | only if maxmind location data is to be loaded; else leave this property unset/blank |
| location.data.country.code.file | only if maxmind location data is to be loaded; else leave this property unset/blank |
| location.data.sub.country.code.file | only if maxmind location data is to be loaded; else leave this property unset/blank |

*Table 29–3  (Cont.) IP Loader Properties*

| IP Loader Properties | Description |
|---|---|
| location.loader.database.pool.size | number of threads to use to update the database |
| location.loader.dbqueue.maxsize | Advanced: maximum number of location records to be kept in queue for database threads |
| location.loader.cache.location.maxcount | Advanced: maximum number of location records to be kept in cache, while updating existing location data |
| location.loader.cache.split.maxcount | Advanced: maximum number of location split records to be kept in cache, while updating existing location data |
| location.loader.cache.anonymizer.maxcount | Advanced: maximum number of anonymizer records to be kept in cache, while updating existing location data |
| location.loader.database.commit.batch.size | Maximum number of location records to batch before issuing a database commit |
| location.loader.database.commit.batch.seconds | Maximum time to hold an uncommitted batch |
| location.loader.cache.isp.maxcount | Maximum number of ISP records to be kept in cache |

### 29.4.1.3 Setting Up for Loading MaxMind IP data

Before running the IP location loader, `Blocks.csv` file from MaxMind must be preprocessed with the following commands:

```
$ mv Blocks.csv Blocks-original.csv
$ sed -e 's/\"//g' Blocks-original.csv | sort -n -t, -k1,1 -o Blocks.csv
```

### 29.4.1.4 Setting Up Encryption

Refer to Chapter 2, "Setting Up the Oracle Adaptive Access Manager Environment for the First Time" for information on setting up encryption.

### 29.4.1.5 Loading Location Data

After completing the setup detailed preceding, run the following command to load the location data into the Oracle Adaptive Access Manager database.

1. Set the `JAVA_HOME` environment variable to point to the location of the JDK.

   Make sure the `JAVA_HOME` environment variable is set to the JDK certified for the Identity Management Suite for *11g*.

2. Run the `loadIPLocationData` script.

   From bash shell, execute `loadIPLocationData.sh`

   From Windows command prompt, execute `loadIPLocationData.cmd`

   The command returns 0 when the data load is successful; on failure it returns 1.

## 29.4.2 System Behavior

The IP location loader utility reads the information from the IP location data files (from Quova/Neustar or ip2location or maxmind) to populate the IP location tables in the Oracle Adaptive Access Manager system. The first time the utility is run against a new database, it inserts one or more rows into the `vcrypt_ip_location_map` for each record in the data file. It also creates a new record in `vcrypt_country` for each unique country name in the data file, a new record in `vcrypt_state` for each unique combination of country name and state name in the data file, and a new record in

vcrypt_city for each unique combination of country name, state name, and city name in the data file.

When the IP location loader is run with a new data file against an already populated database, it skips records in the datafile that have matching, identical records in the vcrypt_ip_location_map table. It creates a new row in the vcrypt_ip_location_map for each record in the data file whose FROM_IP_ADDR does not already appear in the database. It updates the rows in the vcrypt_ip_location_map whose FROM_IP_ADDR matches the record in the data file, but has different data in other columns. The loader also creates new countries, states, and cities that do not already exist in the database.

### 29.4.3 Quova/Neustar File Layout

The Quova/Neustar data file is a pipe-delimited ('|') file, with 29 fields on each line, and one record per line. The information in these tables comes from Quova/Neustar's GeoPoint Data Glossary. In the following table, IP represents the vcrypt_ip_location_map table, CO represents the vcrypt_country table, ST represents the vcrypt_state table, and CI represents the vcrypt_city table.

The file layout is as follows:

*Table 29–4    Quova/Neustar File Layout*

| Quova/Neustar Field | Oracle Adaptive Access Manager Field | Description |
| --- | --- | --- |
| Start IP | IP.from_ip_addr | The beginning of the IP range, also used as an alternate primary key on the vcrypt_ip_location_map table. |
| End IP | IP.to_ip_addr | The end of the IP range. |
| CIDR | (not used) | |
| Continent | (not used) | |
| Country | CO.country_name | The country name. |
| Country ISO2 | (not used) | |
| Region | (not used) | |
| State | ST.state_name | The state name. |
| City | CI.city_name | The city name. |
| Postal code | (not used) | |
| Time zone | (not used) | |
| Latitude | CI.latitude | The latitude of the IP address. Positive numbers represent North, and negative numbers represent South. |
| Longitude | CI.longitude | The latitude of the IP address. Positive numbers represent East, and negative numbers represent West. |
| Phone number prefix | (not used) | |
| AOL Flag | mapped to IP.isp_id | Tells whether the IP address is an AOL IP address. |
| DMA | (not used) | |
| MSA | (not used) | |

*Table 29–4   (Cont.)  Quova/Neustar File Layout*

| Quova/Neustar Field | Oracle Adaptive Access Manager Field | Description |
|---|---|---|
| PMSA | (not used) | |
| Country CF | IP.country_cf | The confidence factor (1-99) that the correct country has been identified. |
| State CF | IP.state_cf | The confidence factor (1-99) that the correct state has been identified. |
| City CF | IP.city_cf | The confidence factor (1-99) that the correct city has been identified. |
| Connection type | mapped to IP.connection_type | Describes the data connection between the device or LAN and the internet. See the Connection Type mapping. |
| IP routing type | mapped to IP.routing_type | Tells how the user is routed to the internet. See the IP Routing Type mapping. |
| Line speed | mapped to IP.connection_speed | Describes the connection speed. This depends on connection type. See the Connection Speed mapping. |
| ASN | IP.asn | Globally unique number assigned to a network or group of networks that is managed by a single entity. |
| Carrier | IP.carrier | The name of the entity that manages the ASN entry. |
| Second-level Domain | mapped to IP.sec_level_domain | The second level domain of the URL. For example, Name in www.oracle.com. This is mapped through the Quova/Neustar reference file. |
| Top-level Domain | mapped to IP.top_level_domain | The top level domain of the URL. For example,. com in www.company.com. This is mapped through the Quova/Neustar reference file. |
| Registering Organization | (not used) | |

### 29.4.3.1  Routing Types Mapping

A table for routing types mapping is shown in Table 29–5.

*Table 29–5    Routing Types Mappings*

| Routing Type | Oracle Adaptive Access Manager ID | Description |
|---|---|---|
| fixed | 1 | User IP is at the same location as the user. |
| anonymizer | 2 | User IP is located within a network block that has tested positive for anonymizer activity. |
| aol | 3 | User is a member of the AOL service; The user country can be identified in most cases; any regional info more granular than country is not possible. |
| aol pop | 4 | User is a member of the AOL service; The user country can be identified in most cases; any regional info more granular than country is not possible. |
| aol dialup | 5 | User is a member of the AOL service; The user country can be identified in most cases; any regional info more granular than country is not possible. |

*Table 29–5   (Cont.)  Routing Types Mappings*

| Routing Type | Oracle Adaptive Access Manager ID | Description |
|---|---|---|
| aol proxy | 6 | User is a member of the AOL service; The user country can be identified in most cases; any regional info more granular than country is not possible. |
| pop | 7 | User is dialing into a regional ISP and is likely to be near the IP location; the user could be dialing across geographical boundaries |
| superpop | 8 | User is dialing into a multistate or multinational ISP and is not likely to be near the IP location; the user could be dialing across geographical boundaries. |
| satellite | 9 | A user connecting to the Internet through a consumer satellite or a user connecting to the Internet with a backbone satellite provider where no information about the terrestrial connection is available. |
| cache proxy | 10 | User is proxied through either an internet accelerator or content distribution service. |
| international proxy | 11 | A proxy that contains traffic from multiple countries. |
| regional proxy | 12 | A proxy (not anonymizer) that contains traffic from multiple states within a single country. |
| mobile gateway | 13 | A gateway to connect mobile devices to the public internet. For example, WAP is a gateway used by mobile phone providers. |
| none | 14 | Routing method is not known or is not identifiable in the preceding descriptions. |
| unknown | 99 | Routing method is not known or is not identifiable in the preceding descriptions. |

### 29.4.3.2  Connection Types Mapping

Table 29–6 shows connection types mappings.

*Table 29–6    Connection Types Mappings*

| Connection Type | Oracle Adaptive Access Manager ID | Description |
|---|---|---|
| ocx | 1 | This represents OC-3 circuits, OC-48 circuits, and so on, which are used primarily by large backbone carriers. |
| tx | 2 | This includes T-3 circuits and T-1 circuits still used by many small and medium companies. |
| satellite | 3 | This represents high-speed or broadband links between a consumer and a geosynchronous or lowearth orbiting satellite. |
| framerelay | 4 | Frame relay circuits may range from low to highspeed and are used as a backup or alternative to T-1. Most often they are high-speed links, so GeoPoint classifieds them as such. |
| dsl | 5 | Digital Subscriber Line broadband circuits, which include aDSL, iDSL, sDSL, and so on. In general ranges in speed from 256k to 20MB per second. |

*Table 29–6   (Cont.)  Connection Types Mappings*

| Connection Type | Oracle Adaptive Access Manager ID | Description |
| --- | --- | --- |
| cable | 6 | Cable Modem broadband circuits, offered by cable TV companies. Speeds range from 128k to 36MB per second, and vary with the load placed on a given cable modem switch. |
| isdn | 7 | Integrated Services Digital Network high-speed copper-wire technology, support 128K per second speed, with ISDN modems and switches offering 1MB per second and greater speed. Offered by some major telcos. |
| dialup | 8 | This category represents the consumer dialup modem space, which operates at 56k per second. Providers include Earthlink, AOL and Netzero. |
| fixed wireless | 9 | Represents fixed wireless connections where the location of the receiver is fixed. Category includes WDSL providers such as Sprint Broadband Direct, as well as emerging WiMax providers. |
| mobile wireless | 10 | Represents cellular network providers such as Cingular, Sprint and Verizon Wireless who employ CDMA, EDGE, EV-DO technologies. Speeds vary from 19.2k per second to 3MB per second. |
| consumer satellite | 11 | |
| unknown high | 12 | GeoPoint was unable to obtain any connection type or the connection type is not identifiable in the preceding descriptions. |
| unknown medium | 13 | GeoPoint was unable to obtain any connection type or the connection type is not identifiable in the preceding descriptions. |
| unknown low | 14 | GeoPoint was unable to obtain any connection type or the connection type is not identifiable in the preceding descriptions. |
| unknown | 99 | GeoPoint was unable to obtain any connection type or the connection type is not identifiable in the preceding descriptions. |

### 29.4.3.3  Connection Speed Mapping

Table 29–7 shows connection speed mappings.

*Table 29–7    Connection Speed Mappings*

| Connection Speed | Oracle Adaptive Access Manager ID | Description |
| --- | --- | --- |
| high | 1 | OCX, TX, and Framerelay. |
| medium | 2 | Satellite, DSL, Cable, Fixed Wireless, and ISDN. |
| low | 3 | Dialup and Mobile Wireless. |
| unknown | 99 | Quova/Neustar was unable to obtain any line speed information. |

## 29.4.4  Oracle Adaptive Access Manager Tables

This section contains the tables used by the ETL process

### 29.4.4.1  Anonymizer

The following tables and sequences are used for uploading the Anonymizer data. Make sure the ETL process has sufficient privileges to read and update these tables.

*Table 29–8    Anonymizer Data*

| Name | Table/Sequence |
| --- | --- |
| V_LONG_VALUE_ELEM_SEQ | Sequence |
| VCRYPT_LONG_VALUE_ELEMENT | Table |
| VCRYPT_VALUE_LIST | Table |
| V_VALUE_LIST_SEQ | Sequence |
| VCRYPT_CACHE_STATUS | Table |
| VCRYPT_CACHE_STATUS_SEQ | Sequence |

### 29.4.4.2  Tables in Location Loading

The IP location loader requires read/write access to the following tables:

- VCRYPT_IP_LOCATION_MAP
- V_IP_LOCATION_MAP_SEQ
- V_IP_LOC_MAP_HIST
- V_IP_LOC_MAP_HIST_SEQ
- V_IP_LOC_MAP_SPLIT
- V_IP_LOC_MAP_SPLIT_SEQ
- V_IP_LOC_MAP_SPLIT_HIST
- V_IP_LOC_MAP_SPLIT_HIST_SEQ
- VCRYPT_COUNTRY
- V_COUNTRY_SEQ
- V_COUNTRY_HIST
- V_COUNTRY_HIST_SEQ
- VCRYPT_STATE
- V_STATE_SEQ
- V_STATE_HIST
- V_STATE_HIST_SEQ
- VCRYPT_CITY
- V_CITY_SEQ
- V_CITY_HIST
- V_CITY_HIST_SEQ
- VCRYPT_ISP
- VCRYPT_ISP_SEQ
- V_ISP_HIST
- V_ISP_HIST_SEQ
- V_LOC_LOOKUP
- V_LOC_LOOKUP_SEQ
- V_LOC_UPD_SESS

- V_LOC_UPD_SESS_SEQ

- V_UPD_LOGS

- V_UPD_LOGS_SEQ

- VCRYPT_LONG_VALUE_ELEMENT

- V_LONG_VALUE_ELEM_SEQ

- VCRYPT_VALUE_LIST

- V_VALUE_LIST_SEQ

- VCRYPT_VALUE_LIST_HIST

- V_VALUE_LIST_HIST_SEQ

- VCRYPT_CACHE_STATUS

- VCRYPT_CACHE_STATUS_SEQ

## 29.4.5 Verifying When the Loading was a Success

The loader script returns 0 when the data load is successful; on failure it returns 1.

# Part XII

# Multitenancy

This part of the book provides concepts on multitenancy in Oracle Adaptive Access Manager

It contains the following chapter:

- Chapter 30, "Multitenancy Access Control for CSR and Agent Operation"

# 30

# Multitenancy Access Control for CSR and Agent Operation

This chapter details the multitenancy access control feature of Oracle Adaptive Access Manager. Multitenancy access control is a way to customize the OAAM Administration Console for each organization so that it results in a different experience for administrative users of multiple tenants.

## 30.1 Multitenancy Access Control

Multitenancy refers to a principle in software architecture where a single instance of the software runs on a server, serving multiple client organizations. With a multitenant architecture, each client organization feels as if they are working with a separate customized application instance.

Figure 30–1 shows a multitenancy access control scenario.

*Figure 30–1  Multitenant Access Control Scenario*
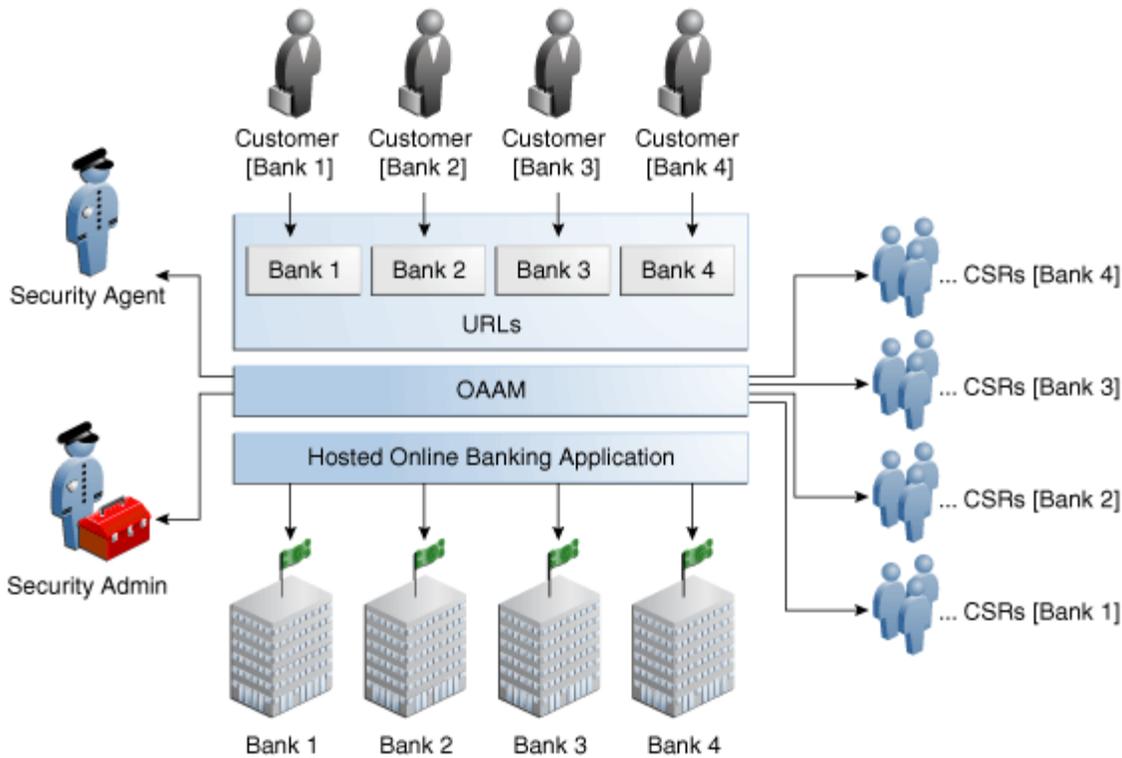


**Application ID**

This is the application request coming from the client (browser). Generally the URL is mapped to an Application ID which is mapped to an Organization ID.

**Organization ID**

Each user belongs to only one Organization ID. It identifies what tenant applications a user utilizes and scopes which OAAM policies will run for them.

**Shared Infrastructure/Shared Application**

In the example shown in Figure 30–1, the online banking application (same instance of the same server) has its data partition in such a way that the application appears different for each client.

**Awareness of the Applications**

The online banking application can be customized by organizations as though each organization had a separate application. Each "application" corresponds to an Application ID: Bank1, Bank2, Bank3, and Bank4.

## 30.2 Mapping of Application ID (Client-Side) to Organization ID (Administration Side)

To ensure that a customer's data is unique from that of other customers, the Application ID is mapped to an Organization ID for use in OAAM Admin.

The Application ID of the client application is mapped to an Organization ID. Users are autoprovisioned to an Organization ID when they access an application for the

first time. For information on mapping applications to Organization IDs, refer to the "*Determining Application ID and User Group*" section of the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

The Application ID is used by OAAM Server to personalize and brand customer pages. They are used by OAAM Admin to determine which set of configuration properties to use to customize the customer applications. For information on customizing user interface branding, refer to the "*Customizing User Interface Branding*" section of the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

From the user's perspective, there is no indication that the (online banking) application is being shared among multiple tenants. When the users access that application, they may go through a specific URL for the bank application or communicate the Organization ID in one of two other ways. OAAM Server can use the URL to display the appropriate pages. Then, the user enters his User ID, which is mapped to an Organization ID.

*Figure 30–2   Mapping of Application ID to Organization ID*
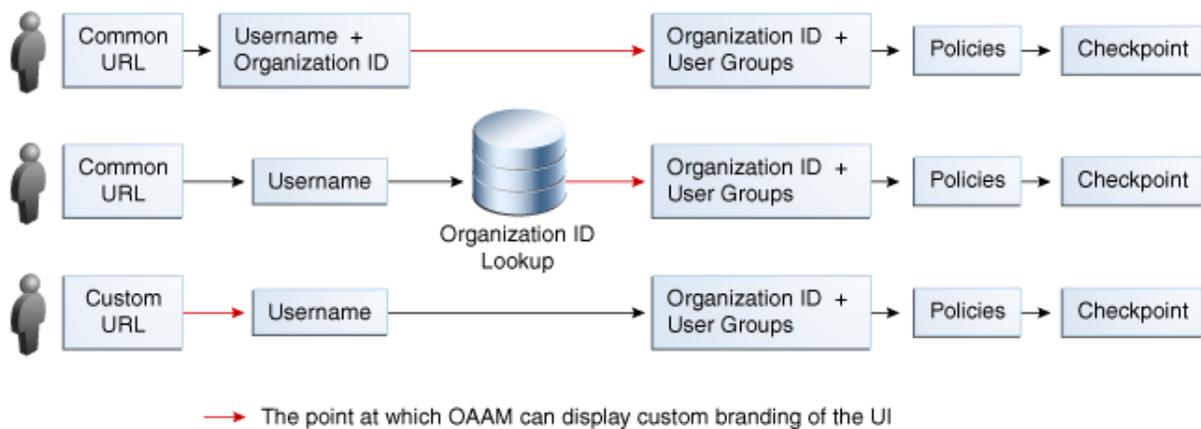


But if banks share a common URL, OAAM Server does not know where users are logging in from; therefore it displays a generic bank screen. OAAM Server can be configured for one of the following scenarios: In example 1, the user enters a User ID and the Organization ID and that combination tells OAAM Server which pages to display. In example 2, the user enters a User ID and through an Organization ID look up OAAM Server is able to determine the correct pages to display. In example 3, the user is directed to the correct screen as soon as he accesses the URL.

# 30.3  Set Up Access Control for Multitenancy

To set up access control for multitenancy, perform the procedures in this session.

## 30.3.1  Set Access Control for Multitenancy

To set up access control for multitenancy, perform the following steps:

1.  In the Properties Search page, specify bharosa.multitenant.boolean as the name to search for.

2.  Click **Search**.

3. Change the value of the bharosa.multitenant.boolean property to true. If you cannot find the property, create it and set it to true.

## 30.3.2 Providing CSR Access to Particular Organizations

To provide access to a particular organization to the CSR administrative user, the CSR administrative user needs to belong to that organization.

At any point, a CSR or CSR Manager can be servicing more than one organization. He will be able to see all the cases of the organizations he is assigned to.

When CSRs are changed or added to an organization, the setting takes effect at the next login and not for the current login.

If you are migrating from a previous release, you can continue to operate as you have been without any change because out of the box, multitenancy access control is off. If you want multitenancy access control, you must set it up. Once you have set up multitenancy, access control is applied. For example, if a CSR belonged to Organization 1 in a previous release, he will still have access to all the cases in Organization 1 after access control is applied. If there is no access control previously, the CSR will have access to all cases. Now if multitenancy access control is set up, he can only see cases from Organization 1. If the CSR was working on five different cases from five different organizations before the upgrade to 11*g*, now he will not have access to them.

### 30.3.2.1 Using WebLogic

To achieve this, an organization with the exact same name as the Organization ID must exist and then that organization should be assigned to the CSR administrative user:

1. Log in to the WebLogic Administration Console as a WebLogic user:

   http://*hostname*:*port*/console

   Where hostname is the hostname of the Administration Server and port is the address of the port on which the Administration Server is listening for requests (7001 by default).

2. Create a group/organization using WebLogic Security Realms that exactly match the name of the Organization ID. For example, Bank1.

   Refer to the "Create groups" section of the Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help 11g.

3. Assign, as necessary/applicable, this group/organization to the CSR and CSR Manager, as necessary.

   Refer to the "Add users to groups" section in the Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help 11g.

To move a user from working on one organization to another:

1. Log in to the WebLogic Administration Console as a WebLogic user:

   http://*hostname*:*port*/console

   Where hostname is the hostname of the Administration Server and port is the address of the port on which the Administration Server is listening for requests (7001 by default).

2. On the Settings for Realm Name page, go to Users and Groups > Users in Security Realms.

**3.** Change the user membership of the group/organization, by removing the group/organization from the CSR and CSR Manager, and adding the new group/organization to the CSR and CSR Manager.

The changes are effective from the next login for the CSR and CSR Managers.

Refer to the "Modify users" section in the Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help 11g.

### 30.3.2.2 Adding Users and Groups to Oracle Internet Directory

If you want to add users and groups through OID, refer to the "Adding Users and Groups to Oracle Internet Directory" in the *Oracle Fusion Middleware Tutorial for Oracle Identity Management*.

### 30.3.2.3 Adding Users and Groups in the LDAP Store

If you want to take care of user and group creation in the external LDAP store, see "Creating Users and Groups for Oracle Adaptive Access Manager" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

## 30.4 What to Expect

This section provides summaries and examples of the multitenant access control experience in OAAM. Multitenancy access control is only applicable for case management data access and filtering on Organization ID and filtering on Session search results. Oracle Adaptive Access Manager cannot control the data administration and security personnel view in the OAAM Administration Console.

*Table 30–1   Multitenant Experiences for CSR and Agents*

| Task | CSR Experience | Agent Experience |
|------|----------------|------------------|
| Create CSR Case | CSRs can select one Organization ID to create a case. | N/A |
| Create Agent Case | N/A | Agents can select one Organization ID to create a case. |
| Search Cases | CSRs can see Organization IDs for which they have access, and from which they can select one (or more) Organization IDs. | Agents can see Organization IDs for which they have access, and from which they can select one (or more) Organization IDs. |
| View Cases | CSRs are able to see the cases from only those organization's users to which they have access. | Agents are able to see the cases from only those organization's users to which they have access. Escalated cases associated with the Organization ID to which agent has access are also included in the search result if it fits the query criterion. |
| Case Details | CSR can see the case detail for cases that belong to any user belonging to an organization he has access to. If the user does not belong to the organization he has access to, the CSR will not see that case in the search results. | Agents can see the case detail for cases that belong to any user belonging to an organization they have access to or cases that are associated with their Organization ID. |
| Case Actions | CSRs can perform case actions on cases they can see. | Agent can perform case actions on a cases they can see. |

*Table 30–1    (Cont.)  Multitenant Experiences for CSR and Agents*

| Task | CSR Experience | Agent Experience |
|---|---|---|
| Sessions Search and Details Pages | CSRs do not have access to sessions search and details pages. | Agent cannot navigate to any of the details pages from sessions page or sessions search if multitenant access control is enabled. If multitenant access control is disabled, Agent is able to access details pages from any sessions search if the link is available. |
| Search Sessions | N/A | Agents can search sessions belonging to the users that belong to the organizations that they have access to and those organizations to which they have access. |
| Search Cases (with changed Organization ID Assignment) | CSR was assigned to "org1." He has created cases created for users in "org1."<br><br>He serviced users for that organization for some time.<br><br>He is then removed from "org1" service and has started servicing "org2."<br><br>When he logs in again after this, he can no longer see the cases for "org1" (whether he created them or not). He can only see and work on the cases that belong to "org2." | Same experience as the CSR. |
| Link Sessions | N/A | Agents can link sessions to the cases belonging to organizations that they have access to.<br><br>Also in search sessions for linking, Agents are able to see the sessions of only those organizations to which they have access. |

## 30.5 Multitenancy Access Control Use Case

The following sections describe examples of common multitenant access control use cases.

### 30.5.1  CSR and CSR Manager Access Controls

Second Bank has deployed OAAM to secure both the consumer banking application and the business banking application. Their CSRs are broken up into two separate organizations. One organization assists only consumer banking customers and the other assists only business banking customers. They need to have strict control over the customer data visible to each of these CSR organizations. Also, there is a organization of senior CSR managers that need to have access to data for all customers. When the consumer banking CSR searches, views, creates, edits cases they only see data related to consumer banking customers. Likewise the business banking CSRs only see data for business banking customers. Neither is even aware that OAAM is doing this pre-filtering of data. The CSR managers can see data related to both consumer and business banking customer activity and they can perform all case flow operations.

**Actors**: CSR and CSR Manager

**Setup**: To set up the scenario:

1. Enable multitenancy access control.

2. Create consumer and business organizations to assist the customers with the exact names as the Organization IDs.

   One organization assists only consumer banking customers and the other assists only business banking customers. They need to have strict control over the customer data visible to each of these CSR organizations.

3. Create CSR1, CSR2, and CSRSenior as administrators.

4. Assign CSR1 to the consumer organization, CSR2 to the business organization, and CSRSenior to both consumer and business organizations.

   To provide access to a particular organization to the CSR administrative user, the CSR administrative user needs to belong to that organization.

   When the consumer banking CSRs (CSR1) search, view, create, and edit cases they only see data related to consumer banking customers. Likewise the business banking CSRs (CSR2) only see data for business banking customers. Neither is even aware that OAAM is doing this pre-filtering of data. The CSR managers (CSRSenior) can see data related to both consumer and business banking customer activity and they can perform all case flow operations.

**Flow**:

1. CSR opens the OAAM Admin Console.

2. CSR sees only the appropriate user interface views and controls afforded his role

3. CSR sees only the appropriate data afforded by his role (Organization ID). He cannot see data for users/sessions related to Organization IDs he does not have permission to view.

4. CSR Manager sees only the appropriate data afforded by his role (Organization ID). He cannot see data for users/sessions related to Organization IDs he does not have permission to view.

## 30.5.2 Agent Access Controls

Second Bank has deployed OAAM to secure both the consumer banking application and the business banking application. Their security analysts are broken up into two separate groups. One group investigates only consumer banking issues and the other investigates only business banking issues. They need to have strict control over all session, policy, and so on, and data visible to each of these security analysts organizations. Also, there is a organization of senior security analysts managers that need to have access to all data. When the consumer banking security analysts searches, views, creates, edits cases they only see data related to consumer banking. Likewise the business banking security analysts only see data for business banking. Neither is even aware that OAAM is doing this pre-filtering of data. The security analysts managers can see data related to both consumer and business banking activity/polices/and so on and they can perform all case flow operations. As well, managers have a filter so they can choose to only view business banking cases/data or only consumer banking cases/data.

Actors: Security Analyst and CSR

**Flow**:

1. CSR/Analyst opens the OAAM Admin Console.

2. CSR/Analyst sees only the appropriate user interface views and controls afforded his role.

3. CSR/Analyst sees only the appropriate data afforded by his role (Organization ID). He cannot see data for users/sessions related to Organization IDs he does not have permission to view.

4. CSR/Analyst Manager sees only the appropriate data afforded by his role (Organization ID). He ca not see data for users/sessions related to Organization IDs he does not have permission to view.

5. CSR Manager can filter what data he sees based on Organization ID.

### 30.5.3 CSR Case API Data Access Controls

Second Bank decides to integrate OAAM with their existing customer ticketing application. They will use the APIs to get customer data and take customer service actions on behalf of customers. Their CSRs are broken up into two separate organizations. One organization assists only consumer banking customers and the other assists only business banking customers. They need to have strict control over the customer data visible to each of these CSR organizations. Also, there is an organization of senior CSR managers that need to have access to data for all customers. The API will allow them to configure the integration to control access to the customer data based on Organization ID to these different groups of employees.

**Actor**: CSR

**Flow**:

1. CSR opens his custom console.

2. CSR sees only the appropriate data afforded by his role (organization ID)

## 30.6 Troubleshooting/FAQ

This section provides information on how to troubleshoot problems that you might encounter when setting up multitenancy access control.

### 30.6.1 I thought I had set up multitenancy access control but CSRs and Investigators still have access to all cases

Verify that you have bharosa.multitenant.boolean set to true. If set to false, multitenancy access control is disabled. By default, multitenancy access control is disabled.

When multitenancy access control is disabled:

- CSRs and Investigators can view and select from all the Organization IDs during case creation.

- In the Cases Home page all Organization IDs are listed for CSRs and Investigators.

### 30.6.2 I have set up multitenancy access control and I have verified that the property is set to true but the CSRs and Investigators are able to access to all cases

You must log out and log back in for access control to be applied. Changing the property takes effect at the next login and not for the current login.

### 30.6.3 Are Security and System Administrators affected when I set up multitenancy access control?

Enabling and disabling multitenancy access control has no effect on users with the security and system administrator roles. Multitenancy access control is only applicable to case management. Their user experience will not be affected.

### 30.6.4 Can CSRs and Investigators have access to multiple organizations?

Yes. They can be assigned to multiple organizations.

### 30.6.5 Can I limit access of a CSR or Investigator to certain organizations even though he had access before?

Yes. Once access control is set up appropriately, the CSR or Investigator will not have access to that Organization ID anymore. He will be limited from accessing the cases of that organization. Changing the property takes effect at the next login and not for the current login.

### 30.6.6 My CSRs and Investigators have no access to cases. What is wrong?

Make sure the CSRs and Investigators are assigned to proper roles and organizations so they can access the cases.

# Part XIII

## Troubleshooting

This part provides information for troubleshooting symptoms and gives solutions to the difficulties you may experience.

# 31

# FAQ/Troubleshooting

This chapter answers common OAAM questions and describes common troubleshooting issues and tips to resolve them.

## 31.1 Techniques for Solving Complex Problems

This section describe a process to enable you to more easily solve a complex problem. It contains the following topics:

- Simple Techniques
- Divide and Conquer
- Rigorous Analysis
- Process Flow of Analysis
- Failures

### 31.1.1 Simple Techniques

You can work your way through some simple troubleshooting techniques to try to solve a problem.

| Steps | Description |
|-------|-------------|
| Experience | You have seen this problem before or it is simply something you know the answer to. |
| Post to the Forum | This is not the first step. Only valid once basics have been applied and a second opinion is needed. Appropriate during rigorous analysis, but not before. |
| Intuitive leap (or guess) | The problem just inspires a guess at a cause. You have a feel for the problem or rather its cause. This can be very effective and result in a quick resolution, but without proper confirmation, it often leads to the symptom being fixed and not the real cause being resolved. |
| Review basic diagnostics | Check the logs for errors and the flow. Check flow (HTTP headers, network packet trace, SQL trace, strace). Run through and document the flow. Cross check with configuration details to ensure flow is expected. |
| Read the error message | Reading the error and the flow information will give a big clue. Taken together with some knowledge of the way the component works, this can give a lot of insight. Always check knowledge (Oracle and search engine) for matches. Perform any diagnostics needed to establish if the error is key. With multiple errors, look to see which is likely the cause and which are just consequences. |

| Steps | Description |
|---|---|
| Compare | Compare the logs and flows with a working system. Perform a test case. If it happens only at a certain site, then compare the differences. |
| Divide | Break the problem down |

## 31.1.2  Divide and Conquer

Steps to reduce the problem to a manageable issue are listed in this section.

| Process | Description |
|---|---|
| Simplify the problem | Make a problem as simple as possible. |
| Remove components that are not needed | Most problems involve complex components and connections between them. Most involve third party components. So where ever possible, eliminate third party components first and then as many components and custom components as possible (for example, command line not application, SQLPLUS is not an application.)? |
| Reduce complexity | Test to see if a simpler version of the problem exists with the same symptoms. (for example, remove components of a complex Select, or a search filter, check if a single request or few requests will suffice)?. |
| Like fixing an underground pipe with a leak | Imagine a complex configuration as being a underground hose pipe with a leak. You know something is wrong, there is a leak someplace, but not where it is. |
| List the components | Draw a box for each components and a line where it is connected to the next. Note the protocols used to join them. |
| Check both ends | What goes in should come out the same. If you see data in and out results in a problem then it is one of the ends that is wrong. If the flow is not as expected the problem is in between. |
| Lazy Y | Test points in the configuration to find where the deviation occurs. Once established (beyond doubt) that a piece of the configuration behaves as expected it can be ignored. |
| Repeat | Repeat this loop to close in on the problem |
| Help | When 3rd party components are involved in the issue, get help from the others and work on the issue together. |

## 31.1.3  Rigorous Analysis

All or part of the process should be applied if:

- a problem is complex

- a problem is highly escalated

- a problem was not solved with the first attempts

- a problem is getting out of control

- a problem has potential for getting out of control

## 31.1.4  Process Flow of Analysis

The process flow of analysis is presented below:

1. State the problem.

2. Specify the problem.

   Develop possible causes from:

       **a.** Knowledge and experience

       **b.** Distinctions and changes

**3.** Test possible causes against the specification.

**4.** Determine most probable cause.

**5.** Verify the solution.

### 31.1.4.1 State the Problem

Stating the problem is the most important step to solving the issue.

| Step | Description |
| --- | --- |
| Ensure a clear and concise problem statement | Stating the problem is the most important step. It is the most commonly ignored or at least the problem statement is assumed. It is pointless trying to solve a problem until the problem statement is stated. Otherwise what are you actually trying to fix? If you do not know what it is you are fixing how can you fix it? |
| Consider if the problem stated can be explained | If so, then it is not the problem statement --If the problem statement can be explained then back up and try and get a more correct problem statement. This is a case to start communicating if you are helping someone solve his problem. Either ask some direct questions to narrow down the issue or just pick up the telephone and talk to the person to clarify the real issue. If there are lots of issues then start noting them down as separate issues. |
| Do not settle for a vague statement | Vague problem statements, like "bad performance", "something crashes" are of no use and commonly are the cause for issues to be long running and out of control. |
| Never combine problems in a single statement | Ensure there is only one problem being dealt with. Do not accept combined problems. The combined problem is either multiple distinct problems or some of the problems are actually symptoms. |

### 31.1.4.2 Specify the Problem

Describe problems in detail and ask focused questions to gather pertinent information.

| Step | Description |
| --- | --- |
| Specify the problem | These are symptoms of the problem. |
| Start by asking questions | Ask questions such as What, Where, When, and to what Extent? |
| What? | **What** tends to be the obvious question and is mostly a list of facts and symptoms; what deviated from the expectation? |
| Where? | **Where** may or may not be relevant, but is worth asking as it is often significant and often overlooked. |
| When | **When** is very important as time lines helps identify patterns and establish what change triggered the problem. |
| Extent | **Extent** or **how many** is particularly useful in establishing probable causes. If it is all the systems for example then check if it affects all systems or try a testcase. How often is also important. Once a week is quite different from many times every second and tells us much about the type of issue to look for. |
| List the symptoms and facts | List the symptoms and facts and how they are significant |
| What changed? | Something changed that is certain unless the problem has always been there. This is a special case. |

| Step | Description |
|---|---|
| Assumptions | Verify the data provided and check for conflicts and contradictions. |
| | Always check for any assumptions. Be careful to identify any information that is not verified and thus is only assumed. In fact this is particularly a mistake made by analysts that have more technical experience. Though also occurs a lot when inexperienced analysts are given details from people they perceive as having more knowledge. However trivial an assumption seems, always look for proof and confirmation. |

### 31.1.4.3 What It Never Worked

If the component did not work before, performing these steps:

| Considerations | Description |
|---|---|
| Consider behavior and expectation if performance issue | For cases when the issue is about something that never worked correctly the first issue is to establish what correct behavior really is and if it is reasonable? This also allows us to set proper expectations from the outset. This is especially true for performance issues. |
| Confirm that there is no misunderstanding | Establish that the requirement is reasonable. |
| Do not compare Apples with Oranges | Agree on a specific goal. Focus on that issue only. |
| Consider all components involved | Consider all components involved:<br>■ Not just the software<br>■ Hardware is fast enough? |
| Consider if the solutions is just to change perception | What can you see that causes you to think there's a problem?<br>■ Human factors<br>■ Perception |

### 31.1.4.4 IS and IS NOT but COULD BE

Consider what the problem is, what it isn't, and what it could be.

| Step | Description |
|---|---|
| IS and IS NOT but COULD BE | For every fact or symptom ask this question: IS and IS NOT but COULD BE |
| Provide comparison | A test case often is the key to establishing something to compare the problem with. |
| | If it reproduces the issue then it does not help the problem analysis as such, but it is extremely useful when passing the problem to the next team to work on the fix. It also allows quicker testing of potential fixes and solutions (workarounds), not to mention you would be gaining experience. |
| If there is no comparison, create a test case | If it does not reproduce then it provides something to compare the problem system with and perhaps even a possible work around. |

### 31.1.4.5 Develop Possible Causes

Problem solving involves developing possible causes.

| Development | Description |
| --- | --- |
| Knowledge and experience | You can use your knowledge and experience to recognize possible causes<br><br>■ Seen before<br><br>■ Seen it in the documentation<br><br>■ Support note or through search engine |
| Distinctions and changes | You can make a list of distinctions and changes to narrow down causes:<br><br>■ Only at this site or on one platform<br><br>■ Just after upgrade<br><br>■ When load increased<br><br>■ Only on Thursdays |
| Examine each of the symptoms and comparisons | Consider each of the facts and ensure that they are relevant and that they are not conflicting |

### 31.1.4.6 Test Each Candidate Cause Against the Specification

Test each candidate cause against the specification:

■ Each possible cause must fit all the items in the specification

■ If you end up with no causes then go back and refine the process

■ Causes must explain both the IS and the IS not but COULD be

■ Determine the most probable cause

■ Do not discount any causes that fit

### 31.1.4.7 Confirm the Cause

Confirm the cause so that you can devise an action plan.

You can:

■ Devise ways to test the possible causes

■ Observe

■ Test assumptions

■ Experiment

■ Test solution and monitor

The main point here is to devise action plans to prove or disprove the theories. It is important to communicate the reason for each action plan. Especially when asking for a negative test, i.e. a test that is to prove something is not true. People might assume all action plans are attempts to solve the problem and resist any thing they think is not directed in the direction.

### 31.1.4.8 Failures

When one solution fails, just start back at the beginning and apply the approach once again, updated with the new results. Really complex problems will often take several iterations.

The process is not infallible.

Main causes of failure are:

- Poor or incorrect problem statement

- Inaccurate or vague information

- Missing the key distinctions in IS vs. IS NOT

- Allowing assumptions to distort judgment

- Not involving a broader set of skills

## 31.2 Troubleshooting Tools

This section contains information about tools and processes you can use to investigate and troubleshoot issues with your system.

Table 31–1 lists the general and OAAM-specific tools you can use for troubleshooting problems.

*Table 31–1    Troubleshooting Tools*

| Category | Description |
| --- | --- |
| General Tools | |
| | <ul><li>Middleware Enterprise Manager</li><li>Database Enterprise Manager</li><li>Monitor Data in DMS</li><li>Audit Data</li><li>Ping/Network Check Tools</li></ul> |
| OAAM Specific Tools | |
| | <ul><li>Dashboard</li><li>Monitor Data</li><li>Log files</li></ul> |

Table 31–2 provides items to check for when troubleshooting the system.

*Table 31–2    Troubleshooting Tips*

| Tips | Reason |
| --- | --- |
| Check the operating system | Some issues may be platform specific. For example, Java keystores created on non-IBM platforms will not work on IBM platforms |
| Check WebLogic Server version | Make sure OAAM is installed on a WebLogic server certified for 11g |
| Check the JDK (Sun or JRockit) | Make sure the JDK is certified for the Identity Management 11g Suite |
| Change logging configuration through Enterprise Manager | Make sure the log level is changed appropriately before tracing and debugging |
| Search for log messages through Enterprise Manager | Log messages record information you deem useful or important to know about how a script executes. |
| Use the Execution Context ID to search for log messages | The ECID is a unique identifier that can be used to correlate individual events as being part of the same request execution flow. |
| Use the WebLogic Console to monitor database connection pool | Check the health of the connection pool through the WebLogic Console. |

Table 31–3 summarizes problems and the checks you can perform to troubleshoot and solve the problem.

*Table 31–3   Problems and Tips*

| Problem | Checks You Can Perform |
|---|---|
| Common Troubleshooting Use Cases | <br>■ Most of the operations are slow<br>■ Server is throwing out of memory exceptions<br>■ Server is throwing encryption related exceptions<br>■ Connection pool related errors occur when starting the server<br>■ Errors while starting managed servers after upgrade<br>■ OAAM CLI script issues<br>■ SOAP call issues<br>■ Native integration issues |
| Most of the Operations are Slow | <br>■ Check performance of OAAM policies<br>   – Use the dashboard to see the performance of the rules<br>   – Tune rules or their parameter if necessary<br>■ Check the database using Enterprise Manager and see if there are any queries that are slow. Follow Enterprise Manager recommendation to add suggested indexes<br>■ Check if the application server CPU is high<br>Take a thread dump if possible<br>■ Check the connectivity and network speed between application server and database<br>■ Use the IP of the database machine in data source settings |
| Server is Throwing Out of Memory Exceptions | <br>■ Check the configuration of the OAAM WebLogic Domain<br>■ See if all the OAAM web applications are deployed on the same managed servers<br>■ Increase the heap size of the managed server |
| Connection Pool Errors | <br>■ Make sure the database listener is running<br>■ Use IP address rather than name in JDBC URL<br>■ Make sure the database service name is correct<br>■ Make sure the connection pool is not too "large"<br>Check if there are too many managed servers accessing the same database |
| Errors While Starting the Managed Server After Upgrade | <br>■ Make sure encryption keys are properly copied<br>■ Make sure all manual steps are followed that are in the upgrade documentation<br>■ Check the WebLogic Console and make sure all web applications are targeted properly to their managed servers |

*Table 31–3   (Cont.)  Problems and Tips*

| Problem | Checks You Can Perform |
|---------|------------------------|
| OAAM CLI Script Issues | |
| | ■ Make sure the JAVA_HOME environment variable is set to the JDK certified for the Identity Management Suite for 11g |
| | ■ Make sure CLI related properties are set in the `oaam_cli.properties` file. |
| SOAP Call Issues | |
| | ■ Known issues exist with time-outs in SOAPGenericImpl |
| | ■ OWSM is enabled by default, so you need to set OWSM policy before using SOAP |
| | ■ Make sure the SOAP server URL including the port number is valid |
| Native Integration Issues | |
| | ■ Make sure the appropriate version of the OAAM Extensions Shared Library is used (the WAR should use the war version and EAR should use the ear version |
| | ■ Make sure the OAAM data source is created and the JNDI name is correct (it should match the JNDI name of the OAAM Server) |
| | ■ Make sure the native application is using the same keys that are used by the OAAM Admin and OAAM server |
| | ■ Issues with the encryption keys |
| |    – Make sure all the managed servers are on the same WebLogic domain or copy the keys across the domains |
| |    – If using non-11g servers, use the Java keystores |
| | ■ Shared library usage by many applications on the same server |
| |    Currently the OAAM Extensions Shared Library cannot be used by more than one application on the same managed server |

## 31.3  Case Management

**Notes in log appear in English**

**Question/Problem**: The notes in the **Logs** tab appear in English.

**Answer/Solution**: The values for the **Notes** column in the **Logs** tab for notes that are not added by the user will appear in English by default.

The notes are taken from the action enums "note" field (property).

The value of that property is saved into database (as notes). After being saved, users cannot change that data.

Implementations can customize the "note" in the enum property to the localized value.

"Access case" is inside the `oaam_resources.properties` file:

```
customercare.case.actiontype.enum.accesscase.description=Access case
```

Case creation / access logic will use that string for the creating records after that point.

## 31.4  KBA

**Why was I challenged with a question I did not register for**

**Question/Problem**: A user states that he was challenged with a question he did not register for. How can this happen?

**Answer/Solution**: There are a few possible reasons:

- The user may have forgotten the challenge questions since registration. Often this is because the user has not been challenged for an extended period.

- The challenge questions may have been reset by another party in a joint account (husband, wife, significant other).

The user's questions should be reset, allowing him to register new challenge questions.

**Should I increase the number of questions for user registration?**

**Question/Problem**: How do I decide if I should increase the number of questions for registration?

**Answer/Solution**: Whether to increase the number of questions depends on the business use case.

If the number of questions is increased to five and the user has three questions registered:

- If the system is using all five questions, you do not need to ask the user to re-register questions. No change is required in this case. Existing users continue to use their questions until the questions are reset.

- If all five questions are required, you can have your users register:

    - An additional two questions, which means you must make changes in the policy and add a new rule

    - All five questions, which means you must use a batch job

**Why is the Question Statistics in the Details Page not displaying the Percentage of Challenges for a Question.**

**Question/Problem**: Why are the statistics not updated for "Percentage of Challenges for a Question" immediately after the user answers a question?

**Answer/Solution**:   The thread which updates the question statistics runs every hour. Updated statistics are not available after a user answers a question. However, the statistics are updated after one hour.

**Level of Answer Logic**

**Question/Problem**: What is the difference between **Off**, **Low**, **Medium**, **High**?

**Answer/Solution**: Answer Logic is a set of advanced matching algorithms used by the system to find out whether the answers provided by the user in the challenge response process match closely to the ones provided during registration. The algorithms and the level of Answer Logic are factors in evaluating answers.

The levels of Answer Logic, the intensity or strength of algorithms, used to evaluate answers are:

- **Off** – No Answer Logic is used; answers must exactly match those previously registered by the user.

- **Low** – Less Answer Logic; answers provided by the user must be a match or near-match to the answers that were provided at the time of registration

- **Medium** – More Answer Logic; the user is given some leeway for the answers that are provided. For example, St. might be accepted for Street.

- **High** – Highest level of Answer Logic. The constraints are not strict for matching.

Refer to Section 7.9.3, "Level of Answer Logic."

### Decryption of user's registered questions and answers

**Question/Problem**: Can a customer decrypt a user's registered questions and answers if needed?

**Answer/Solution**: Decryption of registered questions and answers is not supported for a number reasons. Primarily this is a security concern. If it were supported, it would be possible for an insider to discover the questions and answers for all users. Challenge questions are used to protect applications in times of high risk. These questions in the wrong hands can be used to perpetrate fraud. As well, some KBA answers could contain personally identifiable information which requires a very high level of protection. In addition to security concerns there are privacy concerns as well.

### Are KBA answers case-sensitive?

**Question/Problem**: Are KBA answers case-sensitive?

**Answer/Solution**: KBA answers are not case-sensitive for usability concerns. Since a user will only be challenged with a challenge question when there is a medium level of threat, most users will not be challenged on a regular basis since most users follow regular patterns while conducting their business. If users are not challenged regularly, they may remember the answers to their challenge questions when and if they receive a challenge but may not remember the exact spelling or capitalization. Because of this, KBA includes the use of fuzzy logic to interpret use answers. Common misspellings and abbreviations, for example, can be accepted if the basic information of the answer is correct. This greatly increases the effectiveness as a solution overall since a challenge question is not useful if a user fails to answer correctly because he forgot to capitalize the name of the street he grew up on.

## 31.5 Policies, Rules, and Conditions

### No results were found after policy execution

**Question/Problem**: I imported the policy and expected to see the results from the execution, but no results were found. How can I find out what happened?

**Answer/Solution**: To debug the problem:

1. Check the Session details page to verify if that policy executed in that session.

   Make sure that "vcrypt.tracker.rules.trace.policySet.XXXXXX" is set to true for that checkpoint. (XXXX corresponds to that checkpoint)

2. Verify the configuration of the policy.

   a. Is the policy active?

   b. Is the policy linked to that user group to which this user belongs?

      For a policy to execute in a session, it should either be linked to "All Users" or to one of groups the user is member of. Verify whether the policy is linked appropriately.

**3.** Verify that enough time was given for the cache to refresh.

If group linking is changed recently, make sure to wait more than 30 seconds for the cache to refresh.

### Alerts and/or action did not generate for a rule

**Question/Problem**: The policy executed but alerts and actions were not generated.

**Answer/Solution**: When a rule triggers, the alerts set up in the rule will trigger. However, the action configured in a rule can be overridden in different levels, like trigger combination, policy set override. Look at these for possible override of the action triggered by the rule.

Verify the configuration of actions and alerts.

**1.** Verify that the alerts and actions have been set up in the rule. Then verify that the rule was indeed triggered in the session.

When a rule triggers, the alerts set up in the rule will trigger. However, the action configured in a rule can be overridden in different levels, like trigger combination, policy set override. Look at these for possible override of the action triggered by the rule.

**2.** Verify if there are other trigger combinations in the policy that match this specific set of conditions.

Trigger combinations are evaluated in a sequential order, as shown in the user interface, until all conditions match for a combination. After finding a matching combination, the rest of the combinations are not evaluated. It is possible that multiple combinations match for a specific set of conditions; however only the first one to match will trigger. Verify if there are other trigger combinations in the policy that match this specific set of conditions.

## 31.6 Groups

### Action element or action member does not appear in the action group in rules

**Question/Problem**: An action element was added or an action member, but it does not appear in the action group in rules.

**Answer/Solution**: For the action to appear, you must restart the server because action members are enumerations.

### Unable to delete all the groups

**Question/Problem**: The user is not able to delete all the groups that were selected for deletion.

**Answer/Solution**: If a group is used in other instances within the application, the user will not be able to delete the groups

### Delete all the members in a group

**Question/Problem**: What happens if I delete all the members in a group?

**Answer/Solution**: If the group is linked to any rules or patterns, the rules or patterns will not function as expected.

### Difference between a User ID and a User Name group

**Question/Problem**: What is the difference between a User ID and a User Name group?

**Answer/Solution**: The user name is set up by the user. For example: "Bob" is the login and the user is "xyz123". The User ID is the scheme a customer uses to uniquely identify users.

### Groups Usage

**Question/Problem**: What are groups used for?

**Answer/Solution**: To simplify the configuration for rule conditions and rule results, groups are created.

For example, to create a rule "Restricted IPs," you must add a condition to find out if the logged in user IP is in the list of restricted IPs configured. The restricted IPs are grouped together as RestrictedIPSGroup of type IP and the rule condition will use this group.

### Add/remove group members based on a rule triggering

**Question/Problem**: Can I automatically add/remove members to a group based on a rule triggering? How?

**Answer/Solution**: To add members to a group or remove members from a group, create a new trigger action enumeration named "add member to group" or "remove member from group" and an action group for it. In the group add an action. Configure a configurable action to trigger on "add member to group" or "remove member from group" which will add or remove the member.

### Exclude users

**Question/Problem**: How can I exclude some users from being affected by a rule?

**Answer/Solution**: Create a group which contains the users. Then specify in the Rule's Pre-Condition tab to exclude the group.

### What is a Cache Policy?

**Question/Problem**: What does Cache Policy do?

**Answer/Solution**: The Cache Policy determines if the application uses data stored in the cache or re-fetches original data from the server.

### How does Cache Policy affect performance

**Question/Problem**: How does Cache Policy affect performance?

**Answer/Solution**: Performance is impacted if the application has to consult the server every time the information must be accessed. With cached data, the information is already stored for rapid access. Performance is impacted if you cache data and large changes are made since caching uses server space.

### Not caching a group

**Question/Problem**: In what situations should I not cache a group?

**Answer/Solution**: You should not cache a group if you have a long list of elements since groups are re-cached if there are any changes to the group.

### Group inside a group

**Question/Problem**: Can I have a group inside another group?

**Answer/Solution**: No, the only exception is when a city group could be in a state group which could be in a country group.

### View group linking

**Question/Problem**: How can I see if a group is linked to something else?

**Answer/Solution**: The Policy Tree shows the linking of User ID groups to policies.

## 31.7 Location Loader

### Characters added during transfer of files

**Question/Problem**: During the transfer/ftp of files, characters such as carriage return "\r" are added.

**Answer/Solution**: To resolve the issue, run dos2unix against the files. When you are running the .sh file, use either dos2unix <filename> or dos2unix . *.* .

### TNS:no appropriate service handler found" error

**Question/Problem**: The following error when I load data

```
TNS:no appropriate service handler found
```
**Answer/Solution**: It may be that the number of processes in your database is set to a minimal value.

Use the following commands to check the number of process set in the database

```
SQL> show parameter process
SQL> alter system set processes=100 scope=spfile;
```

## 31.8 Autolearning

### Verify that autolearning is functional

**Question/Problem**: I enabled autolearning and configured the policies. How do I verify that autolearning is running?

**Answer/Solution**: To verify if autolearning is turned on and working:

1. Log in to the system.

2. Run a few logins.

3. To find out whether autolearning data of a session has been processed, go to the Session Details page of that session and view the Processing Status field in the Login Details section.

*Figure 31–1  Autolearning processing*
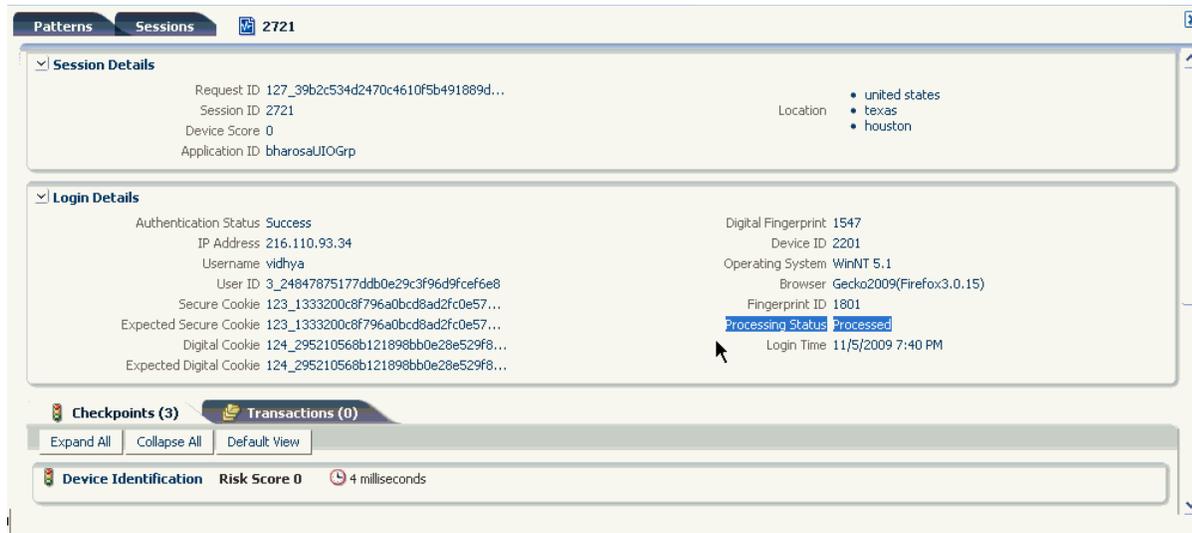


If autolearning has not been set up correctly, data will not have been processed.

## 31.9 Configurable Actions

### Custom action not available

**Question/Problem**: A custom action was created, but it is not available in the user interface.

**Answer/Solution**: Ensure that the Java class is in the right directory and that it is in the right package.

### Multiple cases were generated because of configurable action

**Question/Problem**: Multiple cases are generated when create cases was defined as a configurable action.

**Answer/Solution**: If the pre-condition is an action that can occur frequently, every time, the action occurs, a case is created. For example, actions such as "challenge" can occur more than once in a session (OTP challenge, KBA challenge, and so on).

### Synchronous Actions

**Question/Problem**: Synchronous actions are executed in the order of their priority in the ascending order. For example, if you want to create a CSR case and then send an email with the Case ID, you would choose synchronous actions. Synchronous actions will trigger/execute immediately.

What happens if the first action fails. Will the email be sent still?

**Answer/Solution**: The execution of configurable action is not dependent on the execution of other configurable actions. However, custom code can check data in the context that is shared across actions and perform logic based on the context data.

### Asynchronous Actions

**Question/Problem**: Asynchronous actions are queued for execution and will be executed based on their priority but not in any particular sequence. For example, if you want to send an email or perform some action and do not care about executing it

immediately and are not interested in any order of execution, you would choose asynchronous actions.

Are asynchronous actions guaranteed to execute? What happens if the server stops running?

**Answer/Solution**: If the server stops running, then any pending configurable actions will not be executed.

### Trigger Criteria

**Question/Problem**: Trigger criteria enables you to choose when you want to trigger the action in the session.

The action could be either a score or an action or both. These are compared against the values from the Rule Engine for the selected checkpoint while defining the configurable action.

What happens if both action and score are specified and only one is matched? What is the priority?

**Answer/Solution**: When both action and score are specified, the configurable action is executed only if both of criteria match with the outcome from the Rules Engine.

### Action Priority in Asynchronous Actions

**Question/Problem**: How is action priority used in asynchronous actions?

**Answer/Solution**: Actions are aligned in different queues based on the action priority. When it is time to execute the next action from the queue, the highest-priority action is executed first.

## 31.10  Entities

### Entity not available

**Question/Problem**: A user creates an entity, but it is not available in the Transactions Page Entities list.

**Answer/Solution**: The user has forgotten to activate his entity.

Refer to Section 20.9, "Activating Entities."

### Data element not available for evaluation

**Question/Problem**: The Data element is not available for evaluation in the condition

**Answer/Solution**: The Data element may be encrypted.

### Add multiple entity instances

**Question/Problem**: Can a user add multiple instances of the entity to a Transaction?

**Answer/Solution**: Yes

### Entity change affects instances of the entity

**Question/Problem**: If a user changed the entity definition, are all the instances of the entity affected?

**Answer/Solution**: Yes, the definition is a template

Refer to Section 20.6, "Editing the Entity."

**Not able to delete an entity**

**Question/Problem**: The user is not able to delete an entity. The user has removed that instance from the Transaction already.

**Answer/Solution**: The entity is also used in other transactions, patterns, and so on.

Refer to Section 20.11, "Deleting Entities."

**Not able to delete the entity even when transactions are not using them**

**Question/Problem**: The user does not have any Transaction that uses the entity, but is still not able to delete the entity.

**Answer/Solution**: There might be historical Transaction data using the entity

# 31.11 Transactions

**Group of floating point numbers**

**Question/Problem**: I want to see if the transaction amount is one of a specific value - like $999.99. Is there a way to model this? "Generic Integer" and "Generic Long" are available, but they do not take floating point numbers.

**Answer/Solution**: Where decimals are needed, model by changing the unit. For example, instead of 99.99, use 9999. Care should be taken to use the unit (for example cents instead of dollars) consistently in all the rules and groups.

**Exclude certain entities**

**Question/Problem**: How do you exclude certain entities - like merchants or accounts? For example, merchants and accounts are modeled as entities and Oracle Adaptive Access Manager does not have a "group of entities" option.

**Answer/Solution**: Group the entities using their "primary key" (like a generic strings group.

# 31.12 Jobs

**Question/Problem**: After I execute the task and view the historical data in the dashboard, will there be any difference in the user interface. Will monitor data rollup have an impact on the dashboard?

**Answer/Solution**: There should be no impact on dashboard. There should not be any impact with default settings for cutoff time. If you the set cutoff time to smaller than default, then you may see impact on dashboard. Example: if you perform a daily rollup and change the cutoff time from 3 to 1, then you will lose some of the hourly granularity in the hourly trending view in the bottom part of the dashboard.

# 31.13 Dashboard

**KBA Challenge and Challenge Statistics Do Not Match in Sessions for Time Range**

**Question/Problem**: The Summary Dashboard statistics for KBA challenges does not match the Challenge statistics on the Sessions Search page for the same time range.

**Answer/Solution**: The counts are two different metrics. The Challenge statistics are a count of the number of sessions that were challenged. The KBA Challenge statistics are a count of the number of times a user answered a challenge question.

For example, if a user logs in and is challenged and answers the question incorrectly once, and then answers the question correctly. There will be one session on the Sessions Search page related to this login, but the KBA Challenges on the dashboard will increase by 2.

**The Count of Unsuccessful Challenges is Incorrect in the Summary Logins Report**

**Question/Problem**: A high-risk user logs in to OAAM Server and he is challenged. He enters incorrect answers for the challenge questions. The CSR checks the Oracle Adaptive Access Manager Login Summary Report and looks at the unsuccessful challenges. The count is more than the actual.

**Answer/Solution**: The totals shown in Successful Challenges and Unsuccessful Challenges are the number of times a challenge question was answered successfully or unsuccessfully.

**Average Processing Time for Rules and Policies Does Not Match with Reports**

**Question/Problem**: The CSR captures the rules processing times from session details for a user and runs a SQL query to gather the statistics from the database. The report and SQL query numbers are different than those displayed by the dashboard.

- The average processing times in sessions details and the database are different from the numbers displayed in the performance dashboard. They do not match exactly.

- Execution counts shown in the Dashboard vary from the Security RulesBreakdown report. Additional rules are displayed in the dashboard. (Session details and the Security RulesBreakdown report show fewer rules.)

**Answer/Solution**: The reasons for the mismatch are listed as follows:

1. The execution count shown in the Dashboard and in the Security RulesBreakdown report vary because the dashboard displays the number of times the rule was processed, whether or not they triggered, but the Security RulesBreakdown report displays the number of times the rule returned true. The values in the dashboard and the values returned by that SQL query are different measurements, so the values should not be expected to match.

2. The average processing times in sessions details and the database are different from the numbers displayed in the performance dashboard. They do not match exactly. The monitor data calculates the processing time differently from the report and query. The report and query includes setup code and other processing times not included in the monitor data number. The monitor data contains the rules processing time and the time spent for fact assertions into the working memory.

## 31.14 Command-Line Interface

**Command-Line Errors**

**Question/Problem**: How do I troubleshoot command-line errors?

**Answer/Solution**: Here are the steps to troubleshoot command-line errors:

1. Check Java Version. Make sure it is the same as recommended version. For example, like JDK 1.6.

2. Make sure the jars are in class path (jps*.jars).

3. Define credentials in the Credential Store. The Credential Store is similar to sessions.xml, but the definition is in Enterprise Management for OAAM domain instead of a file.

4. Make sure the SID is correct.

**Schedule exports**

**Question/Problem**: Can I write a CRON job to schedule policy, group, and rule exports?

**Answer/Solution**: Yes.

Steps to create a scheduled job are:

1. Create a script using CLI to export the required data. Test for accuracy of data.

   Refer to Chapter 29, "Oracle Adaptive Access Manager Command-Line Interface Scripts" for information on exporting policies and groups

2. Create a cron job to periodically run the script.

3. Ensure that you:

   a. Encrypt the database password. Refer to Chapter 29, "Oracle Adaptive Access Manager Command-Line Interface Scripts."

   b. Do not overwrite files - Devise a unique naming convention.

   c. Monitor the backup process - Setup email and notification

   d. Monitor disk space /performance - Include only required data in backup, and look for groups with many elements, and so on.

## 31.15 Import/Export

**Importing large policy ZIP files**

**Question/Problem**: I tried to import a large policy ZIP file that contains many policies (the file size is larger than 1MB), but the import failed. The log file does not shows any errors. How can I import this file?

**Answer/Solution**: If OAAM Admin is installed on the Windows platform, you must create a \tmp folder in the drive where you have installed WebLogic.

For example, if the WebLogic domain is on the C drive, you must create a c:\tmp folder.

This folder will be used as a temporary folder for uploading large files into OAAM Admin.

**OAAM Admin failed to import policy, rule condition, and challenge questions ZIP files.**

**Question/Problem**: OAAM Admin failed to import policy, rule condition, and challenge questions ZIP files.

**Answer/Solution**: This is an issue with Mozilla Firefox MIME type mapping. If the environment does not have any application mapped to the ZIP extension, Mozilla maps the incorrect content type. One workaround is to add a file type mapping in Firefox Preferences.

**Browser does not recognize the files which are being uploaded**

**Question/Problem**: When I try to import my Oracle Adaptive Access Manager files, my browser does not recognize them.

**Answer/Solution**: When the MIME entry for Modzilla Firefox is not present in the operating system on which it is installed, the browser fails to recognize correct file types.

A MIME entry must be added for all the types of files, viz, doc, txt, zip, and others under the /etc/mime.types file of any operating system to enable browsers to recognize the files which are being uploaded. Once this entry is there, the browser recognize the files successfully.

There is no issue if the MIME entry is already present in operating system.

## 31.16 Database

**RCU schema load for Oracle Adaptive Access Manager partition does not create tablespace with prefix**

**Question/Problem**: Loading the Oracle Adaptive Access Manager partition schema through RCU does not create tablespaces for the partition using the prefix used in RCU.

**Answer/Solution**: There is a limitation in RCU for only 5 additional tablespace support and 30+ tablespaces are needed for the Oracle Adaptive Access Manager partitioned based schema. Prefixes cannot be used for tablespace names.

**Database Queries to Determine the Space Used**

**Question/Problem**: What are the database queries to use to determine the space used?

**Answer/Solution**:  Use the following databases queries:

The following query can be used to determine average size of row in tables:

```
.
select table_name,
        avg_row_len
   from   user_tables
.
```

The following query can be used to determine size of indexes of the tables:

```
.
   select inds.table_name,
        inds.index_name,
        sum( inds.sizes ) as index_bytes_per_row
   from   (
         select i.index_name,
                i.table_name,
                i.column_name,
                decode(data_type, 'DATE'    , 7,
                                  'CHAR'    , data_length,
                                  'VARCHAR2', decode(
sign(data_length)-250, -1, .7*data_length+3, .7*data_length+1),
                                  'NUMBER'  ,
floor(nvl(data_precision,38)/2)+2 ) as sizes
         from   user_ind_columns i,
                user_tab_columns t
```

```
                 where  t.TABLE_NAME = i.table_name AND
                        t.COLUMN_NAME = i.COLUMN_NAME
              order by i.table_name, i.column_name
            ) inds
      group by inds.table_name, inds.index_name;
```

## 31.17 Monitoring Performance

**Monitoring Performance through Fusion Middleware Control**

You can use Fusion Middleware Control to monitor Oracle Adaptive Access Manager performance and activity.

1. Select OAAM under **Identity and Access** to go to the home page.

   On the home page, you can view a performance overview for Oracle Adaptive Access Manager.

2. Select **Performance Summary** from the Oracle Adaptive Access Manager menu in the upper left hand side of the home page to view performance metrics.

For information on monitoring status and performance with Fusion Middleware Control, see "Monitoring Oracle Fusion Middleware" in the *Oracle Fusion Middleware Administrator's Guide*.

**Monitoring the Security Effectiveness of Oracle Adaptive Access Manager**

The effectiveness of Oracle Adaptive Access Manager can be viewed in multiple ways:

1. Oracle Adaptive Access Manager contains a real-time dashboard of metrics including security actions taken

   For information, see Chapter 24, "Using the Dashboard."

2. OAAM Admin also allows visibility into activity down to the object level details and relationships

   For information, see Chapter 3, "Oracle Adaptive Access Manager Navigation."

3. Oracle Adaptive Access Manager ships with an extensive package of reporting templates for Oracle Business Intelligence Publisher.

   For information, see Appendix D, "Oracle Adaptive Access Manager Reports Reference."

## 31.18 Audit and Query

**Question/Issue**: If I want to query / audit data, it will have to be via the production instance of OAAM using OAAM Admin. This might affect the performance of OAAM Server, since query and audit activities tend to perform many sequential reads / table scans on the production index/tablespaces. How might I lessen the performance impact?

**Answer/Solution**: You might consider maintaining a logical standby database using DataGuard where you can have an option to query / audit / perform reporting using the logical standby database. The logical standby database would have all the data as production, except for the last one hour. The production database instance can just be used to perform its inserts, updates, and so on, and also for active monitoring and alerts.

## 31.19 Archive and Purge

**Registration of "safe" device**

**Question/Problem**: Does running the purge process remove registration of "safe" device?

**Answer/Solution**: There is no special treatment for safe device. Active Devices will not be purged.

Examples are:

6 Months device purge policy

- Device is safe not used in last 6 months - candidate for purge

- Device is not safe and not used in last 6 months - candidate for purge

- Device is safe and used within last 6 months - not candidate for purge. It will not be purged even if device is created more than 6 months back.

- Device is not safe and used within last 6 months - not candidate for purge. It will not be purged even if device is created more than 6 months back.

## 31.20 Device Registration

**Device Registration**

**Question/Problem**: The user has an option in the challenge questions registration page to register a device:

"Check to register the device that you are currently using as a safe device"

If he skipped during the registration flow, he does not seem to have an option later on from the user preferences page. Is there a way to turn it on?

**Answer/Solution**: Device registration is set up to ask the user to register the device during registration and when being challenged.

You can turn it on in the register questions page of user preferences by setting:

bharosa.uio.default.userpreferences.questions.registerdevice.enabled=true

Currently the central user preferences page only allows for unregistering devices.

The user can register the device during registration, but he is also given the option to register the device when being challenged.

## 31.21 Time Zones

**Time zone management**

**Question/Problem**: Do rules that evaluate time use one time zone for all sessions or does it use the time zone from the customer browser/OS? For example, if I set up a rule to KBA challenge if a user logs in outside of office hours (not 8:00 am - 6:00 pm) is this evaluated based on the time zone from the customer browser/OS?

```
Nameuser.timezoneTypeSystemValuePST8PDT
user.timezone = PST8PDT
oaam.adf.timezone = user.timezone
```

The Date and Time used for rule execution (pattern or non-pattern) comes in from "request_time." This is the same date / time that any request based rules will use.

- For on-line it is the OAAM Admin server time.
- For off-line: it is the time specified in the off line data for that request.

## 31.22 Encryption

**How many keystores are there?**

**Question/Problem**: How many keystores are there? And which one is used for what?

**Answer/Solution**: There are 3 keystores:

- System Keystore: Used for encrypting properties and other non database-related data
- Database: Columns in the database. Mostly password, PIN, Transaction data (like credit card #, etc.)...
- SOAP/WebServices: On the client side to authenticate Web Services request

**What tables and columns are encrypted**

**Question/Problem**: If the database is encrypted with these keystores which database tables, or columns, or both are encrypted?

**Answer/Solution**: VCryptPassword and Transaction tables.

**Decrypt data**

**Question/Problem**: Do you need to decrypt the data? When do you need to do this?

**Answer/Solution**: Data is decrypted by the application as and when required. There are not external tools available to decrypt this data.

**Omit encryption**

**Question/Problem**: Can you omit the encryption?

**Answer/Solution**: SOAP is optional. Database and System are mandatory

## 31.23 Globalization

**Characterset in database for Oracle Adaptive Access Manager**

**Question/Problem**: A client already has a database with no UTF8 support, and he wants to keep it that way as it is a shared database and ignore browser locale preferences.

**Answer/Solution**: Since Browser preferences cannot be controlled, the server should ignore Locale preference or always use English.

## 31.24 Localization

**Turn on/off localization**

**Question/Problem**: How do I turn off localization?

**Answer/Solution**: There is no flag to turn-off localization, but there is a user-defined enum that captures the locales supported by the deployment. The enum can be used to enable only one locale.

You would change the `locale.enum.XXX.adminSupported` and `locale.enum.XXX.enabled` properties to `false` for each unwanted locale.

**Language setting on a per user basis?**

**Question/Problem**: Does Oracle Adaptive Access Manager support language setting on a per user basis?

**Answer/Solution**: Usually, Web applications take the language setting of the browser.

For example, a user registers his virtual authentication device and KBA questions using a Spanish browser. If he logs in using an English browser, his phrase will be in Spanish and answers to any KBA questions presented will be expected in Spanish. The KBA question presented to him however will be in English as is expected with most Web application content.

In Oracle Adaptive Access Manager 10.1.4.5 the end-user facing Web application used in proxy type deployments has globalization support. The end user's browser language/locale setting tells the application what language to display the screens in, including KBA questions and the personalization of the virtual authentication devices (phrase). The APIs for KBA and the virtual devices accept locale as a parameter.

However, if the deployment is using native application integration, the functionality would need to be developed in the custom end user facing Web application being built. This application would probably use resource bundles. It would also need to call the KBA and the virtual authentication device APIs while passing a supported locale as a parameter.

# Part XIV

## Appendixes

This section contains the following reference appendixes:

- Appendix A, "Access Roles"
- Appendix B, "Pattern Processing"
- Appendix C, "Conditions Reference"
- Appendix D, "Oracle Adaptive Access Manager Reports Reference"
- Appendix E, "The Discovery and OAAM Policy Development Processes"
- Appendix F, "Globalization Support"
- Appendix G, "Oracle Adaptive Access Manager Properties"
- Appendix H, "Device Fingerprinting"
- Appendix I, "Setting Up Archive and Purge Procedures"
- Appendix J, "Configuring SOAP Web Services Access"
- Appendix K, "Configuring Logging"
- Appendix L, "Rule and Fingerprint Logging"
- "Glossary"

# A

# Access Roles

The Oracle Adaptive Access Manager users can access functionality based on the roles they are assigned. Oracle Adaptive Access Manager ships the following default administrator roles: support personnel, investigators, security administrators, and system administrators. You can also create new users and assign roles appropriately.

This section summarizes the main user groups, their roles, functionality and level of access in OAAM.

## A.1  Support Representative (Group #1)

Support Representatives (Group #1) have very limited access to the OAAM Administration Console.

*Table A–1    Support Representatives*

| Items | Support Representatives (CSR) have access to these features | Notes |
|---|---|---|
| | Users with the Support Representative role have very limited access to the OAAM Administration Console. | |
| Cases | CSRs have access to search, open and create CSR type cases. There are no outward facing hyperlinks in any of the pages CSRs have access to. They have access to a limited list of actions. They have no access to bulk edit functions on search cases page. | Search cases<br><br>■ They can search for CSR cases; They cannot search for agent and escalated cases<br><br>■ They can search for open and closed cases but they cannot reopen closed cases; They can only add notes.<br><br>■ They can search for expired cases and view details but they cannot perform any actions |
| | | New cases<br><br>■ They can open only CSR cases |
| | | View case details<br><br>■ They can view expired case details<br><br>■ They cannot view escalated cases or agent cases<br><br>■ They can view closed case details and add notes<br><br>■ They can view transactions in sessions tab |

*Table A–1 (Cont.) Support Representatives*

| Items | Support Representatives (CSR) have access to these features | Notes |
|-------|-----------------------------------------------------------|-------|
|       |                                                           | Edit case |
|       |                                                           | ■ They can change case status and severity |
|       |                                                           | ■ They cannot add public notes to Escalated Cases |
|       |                                                           | ■ They cannot bulk edit cases |
|       |                                                           | ■ They can escalate cases |
|       |                                                           | ■ They cannot perform a temporary allow for a user |
|       |                                                           | ■ They cannot OTP bypass users |
|       |                                                           | ■ They cannot extend expiration |
|       |                                                           | ■ All customer and KBA resets |
|       |                                                           | ■ KBA phone challenge |
|       |                                                           | ■ They can perform Customer Resets - a. Image and Phrase. |
|       |                                                           | ■ Challenge Questions |
|       |                                                           | Reset Questions |
|       |                                                           | Reset Question Set |
|       |                                                           | Unlock Customer |
|       |                                                           | Ask Question |
|       |                                                           | ■ Expired status cases - Search Access; No access to open |
|       |                                                           | ■ OTP Actions |
|       |                                                           | Reset Email |
|       |                                                           | Reset Phone |
|       |                                                           | Reset All |
|       |                                                           | Unlock OTP |

## A.2 Support Manager (Group #2)

Groups #2 members will have the access privileges of Group #1 plus some other limited functionality.

*Table A–2 Support Manager*

| Items | Support Managers have access to these features | Notes |
|-------|------------------------------------------------|-------|
|       | Support Managers have the access privileges of the Support Representative and some other limited functionality. | |
| Cases | No create agent type cases. Hide actions, log and linked/related tabs in agent cases | Search Cases<br>■ They can search for CSR, Agent and Escalated cases<br>■ They can search for open and closed cases.<br>■ They can search for expired cases. |

*Table A–2   (Cont.)  Support Manager*

| Items | Support Managers have access to these features | Notes |
|---|---|---|
| | | New Case |
| | | ■ Only CSR cases |
| | | View Case Details |
| | | ■ They can view Escalated Case details (including logs and sessions); but cannot perform any actions |
| | | ■ They can view closed case details (They can only add notes or change status) |
| | | ■ They can view Transactions in sessions tab |
| | | ■ They can view expired case details (They can only add notes and extend expiration date) |

*Table A–2   (Cont.)  Support Manager*

| Items | Support Managers have access to these features | Notes |
|---|---|---|
| | | Edit cases |
| | | ■   They cannot perform any actions on Escalated Cases |
| | | ■   They can |
| | | Re-open closed cases |
| | | Add notes in CSR cases |
| | | Change status and severity |
| | | Bulk edit CSR cases |
| | | Escalate cases |
| | | Grant temporary allow to users |
| | | OTP bypass users |
| | | Extend expiration |
| | | Perform all customer and KBA resets |
| | | Perform KBA phone challenge |
| | | Change Status |
| | | Change Severity |
| | | ■   Temporary Allow |
| | | Single login |
| | | 2 hours |
| | | Set end date |
| | | ■   Customer Resets |
| | | Image |
| | | Phrase |
| | | Image and phrase |
| | | Customer (all) |
| | | ■   Challenge Questions |
| | | Unlock Customer |
| | | Reset Questions |
| | | Reset Question Set |
| | |  Next Question |
| | | Ask Question |
| | | ■   Closed status cases - Search and open Access |
| | | ■   Expired status cases - Search and Open Access |
| | | ■   Escalate a CSR case - Full Access |
| | | ■   Link Sessions tab in escalated status |
| | | ■   OTP Actions |
| | | ■   Can search for and view session details; but no access to detail pages or policy explorer |

## A.3  Fraud Investigator

Fraud Investigators have wide access to the OAAM Administration Console.

*Table A–3    Fraud Investigator*

| Items | Group has access to these features | Notes |
|---|---|---|
| | Fraud Investigators have wide access to the OAAM Administration Console. | |
| | | Also access to add /remove/delete group memberships from details pages |
| Navigation Tree | Full Access (ready only except environment) | ■ No access to bulk editing of cases.<br>■ Full access for CSR, Agents and Escalated cases |
| Cases | Full access. | |
| Search page | Search Agent Cases | |
| Scheduler | No access | |
| Environment | No access | |

## A.4  Fraud Investigation Manager

Fraud Investigation Managers have wide access to the OAAM Administration Console.

*Table A–4    Fraud Investigation Manager*

| Items | Group has access to these features | Notes |
|---|---|---|
| | Fraud Investigation Managers have wide access to the OAAM Administration Console. | |
| | | Also Access to add /remove/delete group memberships from other pages |
| Navigation tree | Full Access (ready only except environment) | ■ Full access to bulk editing of cases<br>■ Full access to CSR, Agent and Escalated cases |
| Cases | Full access. | |
| Scheduler | No access | |
| Environment | No access | |
| Home Page | Search Agent Cases | |

## A.5  Security Administrator

Security Administrators have wide access to the OAAM Administration Console.

*Table A–5    Security Administrator*

| Items | Group has access to these features | Notes |
|---|---|---|
| | Security Administrators have wide access to the OAAM Administration Console. | |
| | | Except Environment node and security dashboard (should be hidden by default) |
| Navigation Tree | Full Access | Not closable |
| Home Page | Search Policies | |
| Cases | View only access | |
| Scheduler | Access for Offline Security Administrators | |
| Environment | No access | |

## A.6  System Administrator

Limited access to the OAAM Administration Console for system administration duties

*Table A–6    System Administrator*

| Items | Group has access to these features | Notes |
|---|---|---|
| | Limited access to the OAAM Administration Console for system administration duties | |
| | | ■ No access to cases ■ Full access to Environment ■ Read-only access to everything else |
| Navigation Tree | Partial access | |
| Scheduler | Access to Online and Offline System Administrators | |
| Environment | Full access | |
| Home Page | Search Properties | |

## A.7  Auditor

Auditor has no access to the OAAM Administration Console. They will do their audit work in BIP.

*Table A–7    Auditor*

| Items | Group has access to these features | Notes |
|---|---|---|
| | Auditor has no access to the OAAM Administration Console. They will do their audit work in BIP and the common audit framework. | |

# B

# Pattern Processing

Autolearning is the application of several Oracle Adaptive Access Manager features to dynamically profile behavior of user, device, locations, and transaction entities. Patterns are defined by an administrator to automatically capture behavior. These patterns are in turn used by Oracle Adaptive Access Manager to dynamically create and populate buckets based on the pattern parameters. Oracle Adaptive Access Manager automatically records/maintains the bucket memberships of the users/devices/locations/entities over time so that the overall profile can be used to evaluate risk. As well, dynamic actions are used to populate groups based on rule outcomes to further profile behavior. The memberships of these automatically managed groups are also used to evaluate risk.

This appendix provides information about autolearning pattern data processing.

## B.1 Pattern Data Processing

If the system load is light and if the pattern is configured, the data will be processed as soon as the clients calls the API that is used for triggering the data processing. The system load is the number of authentication, transaction, rule processing (and other) reports and requests served by the Oracle Adaptive Access Manager server.

The logic for processing the data is as follows.

For each (successful) transaction record, the following process occurs:

1. Gather all the attributes of the transaction from the database.

2. Determine the transaction type and if any of the patterns have the same transaction type as the one you have at hand.

3. If there are no patterns having the same transaction type as the one at hand, the process is stopped at this point and returns to the caller with nothing.

4. If there are patterns that have the same transaction type as the one at hand, then the following process is performed for each pattern.

   a. Get the parameters for that pattern and determine if the parameter values for the transaction at hand satisfy the requirements (like range for example). If not, move to next pattern.

   b. If the parameters satisfy the requirements, then go to the fingerprint table.

   c. If the fingerprint exists for such a combination, then go ahead and update the counters in workflow tables (hour, day, month, year) for entities added to the pattern.

   d. If the fingerprint does not exist, then create a fingerprint and create entries in the workflow table for that fingerprint and put the count there.

e. After this determine if the pattern is configured to capture the one-time or lifetime values for the parameters, if set to do so. Then go and update the correct profile table. While doing this, if the profile table does not have an entry for this entity, create the entry. Data1 through Data10 fields from entity profile tables will be used to capture the pattern membership and the values.

f. Repeat Steps a through e for rest of the patterns.

5. Repeat Steps 1 through 4 for each transaction.

# B.2 APIs for Triggering Pattern Data Processing

The APIs for triggering patterning data processing are

- updateTransaction

- updateAuthStatus

- processPatternAnalysis

The updateAuthStatus and updateTransaction APIs are similar to other update authentication and transaction status APIs. The only difference is that updateTransaction, updateAuthStatus, and processPatternAnalysis perform pattern data processing in addition to the updating status of authentication or transaction.

## B.2.1 updateTransaction

API to update a previously created transaction.

It also triggers pattern data processing if appropriate. A nonzero value of analyzePatterns will result in triggering the pattern processing if not already performed for this transaction.

```
public VCryptResponse updateTransaction(
                Transaction UpdateRequestData transactionUpdateRequest Data);
```

*Table B–1    updateTransaction Parameter and Returned Value*

| Parameter | Description |
|---|---|
| TransactionUpdateRequestData | The object to update a transaction; a handle to the transaction to be updated is either the Transaction ID returned by the method createTransaction, or the external Transaction ID passed to the method createTransaction. it throws the exception BharosaException if it fails validation.<br><br>The structure of this object is as follows:<br><br>■ requestId, identifies the user session; required<br><br>■ requestTime, the time of the request; can be null; if null, the server uses the current time<br><br>■ transactionId ID, the ID returned by a previous call to createTransaction<br><br>■ status, the transaction status<br><br>■ analyzePatterns, Boolean to indicate if pattern processing should be performed. When the value is passed in as "true," the pattern processing is performed for the transaction if the "resultStatus" value is "success."<br><br>■ externalTransactionId, the external Transaction ID that was passed to createTransaction when the transaction was created |
| VCryptResponse | The response object; make sure to check isSuccess() before obtaining the Transaction ID with the method getTransactionResponse() |

## B.2.2 updateAuthStatus

API to update the user node log auth status and trigger the pattern data processing if appropriate. A value of true for analyzePatterns and a value of "success" for the resultStatus of the transaction will result in triggering the pattern processing if not already performed for this transaction.

- public VCryptResponse updateAuthStatus(java.lang.String requestId, int resultStatus, int clientType, java.lang.String clientVersion, boolean analyzePatterns)

- public VCryptResponse updateAuthStatus(java.lang.String requestId, java.util.Date requestTime, int resultStatus, int clientType, java.lang.String clientVersion, boolean analyzePatterns)

*Table B–2    updateAuthStatus Parameters*

| Parameter | Description |
| --- | --- |
| requestId | Request ID |
| requestTime | Time of update |
| resultStatus | The authentication result. This is the enumeration value of the authentication result. |
| clientType | This is an enum value defined to identify the client type used for authentication. |
| clientVersion | Optional parameter to specify the version of the client used |
| analyzePatterns | Boolean to indicate if pattern processing should be performed. When the value is passed in as "true," the pattern processing is performed for the transaction if the "resultStatus" value is "success." |

## B.2.3 processPatternAnalysis

API to trigger the processing of data for pattern matching. This call will only trigger the processing of data for pattern matching. The last parameter transactionType can be used by the authentication type user interactions, since authentication (or login) are not first-class transactions.

public VCryptResponse processPatternAnalysis(java.lang.String requestId, long transactionId, int status, java.lang.String transactionType)

*Table B–3    processPatternAnalysis*

| Parameter | Description |
| --- | --- |
| requestId | Request ID |
| transactionId | Transaction ID to be updated. |
| status | New Status |
| transactionType | String that indicates the type of transaction. Has to be "auth" for authentication type. For other types it can be "bill_pay, ....",; basically the type name of the transaction. |

# C

# Conditions Reference

This appendix provides information about the conditions available standard on Oracle Adaptive Access Manager.

- **Autolearning Conditions**
  - Pattern (Authentication): Entity is Member of Pattern Bucket for First Time in Certain Time Period
  - Pattern (Authentication): Entity is Member of Pattern Less Than Some Percent Time
  - Pattern (Authentication): Entity is Member of Pattern Less Than Some Percent with All Entities in Picture
  - Pattern (Authentication): Entity is Member of Pattern N Times
  - Pattern (Authentication): Entity is Member of Pattern N Times in a Given Time Period

- **Device Conditions**
  - Device: Browser Header Substring
  - Device: Check if Device is of Given Type
  - Device: Device First Time for User
  - Device: Excessive Use
  - Device: In Group
  - Device: Is Registered
  - Device: Timed Not Status
  - Device: Used Count for User
  - Device: User Count
  - Device: User Status Count
  - Device: Velocity from Last Successful Login

- **Location Conditions**
  - Location: ASN in Group
  - Location: in City Group
  - Location: In Carrier Group
  - Location: In Country Group
  - Location: IP Connection Type in Group

- Transaction: Compare Transaction Counts Across Two Different Durations
- Transaction: Compare Transaction Entity/Element Counts Across Two Different Durations
- Transaction: Check Unique Transaction Entity Count with the specified count

- User Conditions
  - User: Check If Devices Of Certain Type Are Used
  - User: Check User Data
  - User: Stale Session
  - User: Devices Used
  - User: Velocity from Last Success
  - Understanding How the OAAM Device Max Velocity Rule Settings Work
  - User: Check Number of Registered Devices Of Given Type

## C.1  List of Available Conditions

The following table lists the available out of the box conditions.

*Table C–1  Rule Conditions*

| 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: Check if device is of given type | Checks whether the current device is of selected device type. |
| Device: Check if device is using Mobile Browser | Checks whether the current device is using mobile browser to access the site based on the User Agent String |
| Device: Device first time for user | Checks whether this device is used for the first time by this user |
| Device: Device in group | Checks if this device is in group |
| Device: Excessive use | Checks whether device is excessively used but not used before |
| Device: Is registered | Checks if the user has registered this device |
| Device: Timed not status | Checks the maximum login attempts for all but the given status within the given time period |
| Device: User count | Checks the unique user count using this device in past "x" seconds |
| Device: Used count for User | Checks the device used count. This condition ignores the current request for calculating the device count. |
| Device: User status count | Checks the user count with the given status from this device in specified duration |
| Device: Velocity from last login | Triggers when miles per hour is more than specified value and the IP does not belong to ignore IP group |
| Location: ASN in group | Checks whether the ASN for the current IP address is (or is not) in the ASN group |
| Location: Carrier in group | Checks if the IP is in the given carrier group |
| Location: City in group | Checks if the IP is in the given city group |
| Location: Domain in group | Checks if the Second Level Domain is in the group |

*Table C–1   (Cont.)  Rule Conditions*

| Condition | Description |
| --- | --- |
| Location: In Country group | Checks if the IP is in the given country group |
| Location: IP Connection speed in group | Checks if the IP Connection Speed is in the group |
| Location: IP Connection type | Checks the connection type for the IP. The connection type could be DSL, Cable, ISDN, Dialup, Fixed Wireless, Mobile Wireless, Satellite, Frame Relay, T1/T3, OCx, and others |
| Location: IP Connection type in group | Checks if the IP connection type is in the group |
| Location: IP Excessive use | Checks if IP is excessively used but not used before |
| Location: IP in group | Checks if the IP is in the IP group |
| Location: IP in Range group | Checks if the IP is in the IP range specified in an IP Range group. Condition will check if IP of activity belongs to one of the IP ranges specified in the list of ranges. |
| Location: IP is AOL | Checks if the IP is from an AOL proxy |
| Location: IP line speed type | Checks the connection line speed type for the IP. This is categorized into High, Medium, Low or Unknown |
| Location: IP Maximum logins | Checks the maximum number of logins using the current IP address within the given time duration. This condition ignores the current request during evaluation of maximum logins count. |
| Location: IP Maximum Users | Checks the maximum number of users using the current IP address within the given time duration |
| Location: IP Multiple Devices | Checks the maximum number of devices from IP address within the given time duration |
| Location: IP routing type | Checks the 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 | Checks if the IP Routing Type is in the group |
| Location: IP type | Checks if IP is valid, unknown or private |
| Location: Is IP from AOL | Checks if the IP is from AOL proxy |
| Location: ISP in group | Checks if the ISP for the current IP address is (or is not) in the ISP group |
| Location: State in group | Checks if the IP is in the given State group |
| Location: Timed not status | Checks the maximum login attempts for all but the given status within the given time period |
| Location: Top Level Domain in group | Checks if the Top Level Domain is in the group |
| Location: User status count | Check the user count with the given status from this location in specified duration |
| Pattern (Authentication): Entity is a member of the pattern less than some percent of time | Evaluates if the entity of the type specified (user, device, location, and so on) involved in the current access request has been a member of the pattern specified less/more than the defined percentage within the time range configured. |
| Pattern (Authentication): Entity is a member of pattern bucket for the first time in a certain time period | Checks if this Entity is member of pattern bucket for first time in certain time period |
| Pattern (Authentication): Entity is a member of the pattern bucket less than some percent with all entities in the picture | Checks if this entity has been member of this pattern bucket based on percent basis, taking into account all other entities |

***Table C–1   (Cont.)  Rule Conditions***

| Condition | Description |
| --- | --- |
| Pattern (Authentication): Entity is a member of the pattern N times | Checks to determine whether the entity is a member of the pattern more than "n" number of times. This condition is intended to be used only with single bucket type patterns since it evaluates pattern membership as opposed to individual bucket membership. |
| Pattern (Authentication): Entity is a member of the pattern N times in a given time period | Checks if this entity has been member of this bucket. You can compare if this entity has been belonging to this bucket before. |
| Transaction: Check Count of any entity or element of a Transaction using filter conditions | Checks count of any entity or element of a Transaction using filter conditions |
| Transaction: Check Current Transaction using the filter conditions | Checks current transaction using filter conditions |
| Transaction: Check if consecutive Transactions in given duration satisfy the filter conditions | Check if consecutive transactions in given duration satisfy the filter conditions |
| Transaction: Check number of times entity used in transaction. | Compares the number of times an entity used has been used with the specified count. |
| Transaction: Check Transaction Aggregrate and Count using filter conditions | Checks the transaction aggregrate and count using filter conditions |
| Transaction: Check Transaction Count using filter conditions | Checks the transaction count using filter conditions |
| Transaction: Check Unique Transaction Entity Count with the specified count | Checks the unique transaction entity count with the specified count |
| Transaction: Compare Transaction Aggregrates (Sum/Avg/Min/Max) across two different durations | Compares the transaction aggregrates (Sum/Avg/Min/Max) across two different durations |
| Transaction: Compare Transaction Counts across two different durations | Compares the transaction counts across two different durations |
| Transaction: Compare Transaction Entity or Element Counts across two different durations | Compares the transaction entity or element counts across two different durations |
| Session: Check parameter value | Checks if specified parameter value is more than specified value |
| Session: Check parameter value for regular expression | Checks if specified parameter value matches regular expression |
| Session: Check parameter value in group | Checks if specified parameter value is in group |
| Session: Check Risk Score Classification | Checks the risk score classification based on the risk score from previous checkpoint execution |
| Session: Check string parameter value | Checks to compare string value |
| Session: Check two string parameter value | Checks to compare two parameters string value |
| Session: Check value in comma separated values | Checks if specified value is present in comma separated value list. |
| Session: Compare two parameter values | Compares two parameter values |
| Session: Check enough pattern data | Checks if enough pattern data is available for given pattern |
| Session: Check enough any pattern data | Checks if enough pattern data is available in the system for any pattern |
| Session: Check Current Session using the filter conditions | Check Current Session using (up to 5) filter conditions |

**Table C–1   (Cont.)  Rule Conditions**

| Condition | Description |
|---|---|
| Session: Compare with current date time | Compares specified parameter value with current time |
| Session: Cookie Mismatch | Checks to see if there is mismatch of supplied cookie with the expected cookie |
| Session: IP Changed | Checks if IP Address is changed since transaction is started |
| Session: Mismatch in Browser Fingerprint | Checks to see if there is mismatch in browser fingerprint with the fingerprint supplied during authentication. Fingerprint is constructed using the context values passed to Rules Engine |
| Session: Time Unit | Checks if the current time unit matches the specified time unit criteria. |
| System - Check Boolean Property | Checks the system property |
| System: Check if enough data is available for any pattern | Checks if a defined minimum amount of pattern data has been captured in the OAAM database. Generally the threshold should be set to between 1-3 months for best results. The out of the box policies utilize this rule to determine if there is enough pattern data captured to start running pattern based risk analysis. |
| System: Check if enough pattern data is available | Checks if enough pattern data is available. This condition will check if pattern data is available in the system for last several days for a given pattern. |
| System - Check Integer Property | Checks system property |
| System - Check Policy max score | Checks Policy maximum score |
| System - Check Policy min Score | Checks Policy minimum score |
| System - Check Request Date | Checks request date |
| System - Check String Property | Checks system property |
| System - Evaluate Policy | Processes the policy as rule and evaluate results |
| User: Account Status | Checks account status of the user |
| User: Action Count | Checks action counter for the given action. This condition has dependency on action configuration |
| User: Action Count Timed | Checks if the given action count is more than specified count. If checkpoint is not specified, action is checked in all checkpoints |
| User: Action Timed | Checks maximum number of actions in the past "x" seconds |
| User: ASN for first time | Checks if user using this ASN for the first time? |
| User: Authentication Image Assigned | Checks if authentication image is assigned to user |
| User: Authentication Mode | Check user authentication mode |
| User: Challenge Channel Failure | Checks if a user has a failure counter value over a specified value from specific channel |
| User: Challenge Failure Is Last Challenge Before | Checks if it is the last challenge before number of hours, since number of days have passed. |
| User: Challenge Failure - Minimum Failures | Checks if a user has a failure counter value over a specified value. |
| User: Challenge Maximum Failures | Checks if user failed to answer challenge question for specified number of times |
| User: Challenge Questions Failure | Checks how many questions have failures |
| User: Challenge timed | Checks if user answered challenge question successfully in last n days |
| User: Check Anomalous User Request | Checks if the current User Request is Anomalous |

*Table C–1   (Cont.)  Rule Conditions*

| Condition | Description |
| --- | --- |
| USER: Check Devices of Certain Type are Used | Checks if devices of certain type are used for successful sessions within some seconds |
| User: Check Devices Used | Checks the number of devices tried in given time |
| User: Check first login time | Checks if user first logged in within range. First login is the first successful login |
| User: Check Fraudulent User Request | Checks if the current User Request is fraudulent |
| User: Check Information | Checks to see if user information is set. Information data to check is sent as key value pair. |
| User: Check Last Session Action | Checks if the given action is in last session. If checkpoint is not specified, action is checked in all checkpoints of that session |
| User: Check login count | Checks user login count within specified duration |
| User: Check Login Time | Checks if user login time is within the specified time |
| User: Check OTP Failures | Checks if user's OTP failure counter value over a specified value |
| User: Check User Data | Checks User Data for the given key |
| User: Checkpoint score | Checks if the score is within limits |
| User: City first time for user | Checks whether the user is using this city for the first time? |
| User: Client And Status | Checks account status of the user |
| User: Country failure count for user | Checks failure count for the user from the given country |
| User: Country first time for user | Checks if the user is using this Country for the first time? |
| User: Country first time from group | Checks if this country is used for the first time by this user from the given country group |
| User: Distance from last successful login | Checks the distance from last successful login within specified time |
| User: Distance from last successful login within limits | Checks if distance from last successful login within specified time is within limits |
| User: Image Status | Checks the image status of the user |
| User: In Group | Checks if the user is in the given group |
| User: IP carrier for first time | Checks if the user is using this IP carrier for the first time? |
| User: Is last IP match with current IP | Checks if user login IP address matches with that of previous login |
| User: Is User Agent Match | Checks if user agent matches with that of previous login from same device |
| User: Last Login Status | Checks to see if user login status is in specified list |
| User: Last login within specified time | Checks the last login within specified time |
| User: Location Used Timed | Checks if user used this location within the given time period |
| User: Login for first time | Checks if user is logging in for the first time |
| User: Login in group | Checks if the user login is in the given group |
| User: Login time between specified times | Checks the login time between specified time |
| User: Maximum Cities | Checks the number of cities within the given time period |
| User: Maximum Countries | Checks the number of countries within the given time period |
| User: Maximum IPs Timed | Checks the maximum number of IP within the given time period |

**Table C–1   (Cont.) Rule Conditions**

| Condition | Description |
| --- | --- |
| User: Maximum Locations Timed | Checks the maximum number of locations within the given time period |
| User: Maximum States | Checks the number of states within the given time period |
| User: Multiple failures | Checks if user failed multiple times |
| User: Check Number of Registered Devices Of Given Type | Number of registered devices of given type. |
| User: Phrase Status | Checks phrase status of the user |
| User: Preferences Configured | Checks if the user preferences are set |
| User: Question Status | Checks Question status of the user |
| User: Stale session | Checks if a newer session was established after this session is created |
| User: State first time for user | Checks if the user is using this state for the first time? |
| User: Status Count Timed | Checks if user attempted multiple logins in specified time |
| User: User Agent Percentage Match | Checks if user agent percentage match is above specified percentage. Compares with browser user agent string (UAS) of previous login from same device |
| User: User Carrier for first time | Checks to see if the user has used this Carrier successfully previously |
| User: User City for first time | Checks to see if the user has used this City successfully previously |
| User: User Country for first time | Checks to see if the user has used this Country successfully previously |
| User: User Group in Group | Checks if the user group is in the given group |
| User: User IP for first time | Checks if the user has used this IP successfully previously |
| User: User ISP for first time | Checks if the user has used this ISP successfully previously |
| User: User is member of pattern N times | Checks if this user has been member of this pattern Condition |
| User: User state for first time | Checks if the user has used this state successfully previously |
| User: Velocity from last successful login | Checks the velocity from last successful login |
| User: Velocity from last successful login within limits | Triggers when velocity from last successful login is within specified limits |

The following table lists the device fingerprinting policies.

**Table C–2   Device ID Policies**

| Condition | Description |
| --- | --- |
| Device ID: Cookies match | Checks if tracker node matches for both cookies |
| Device ID: Cookie state | Checks the cookie state for the given device and user |
| Device ID: Header data match | Checks if header data match |
| Device ID: Header data match percentage | Checks if header data match percentage is within specified range |
| Device ID: Header data present | Checks if header data is present |
| Device ID: HTTP header data browser match | Checks if browser is matched based on HTTP header data |
| Device ID: HTTP header data browser upgrade | Checks if browser is upgraded based on HTTP header data |

**Table C–2    (Cont.)  Device ID Policies**

| Condition | Description |
|---|---|
| Device ID: HTTP header data OS match | Checks if OS match based on HTTP header data |
| Device ID: HTTP header data OS upgrade | Checks if OS is upgraded based on HTTP header data. Check is based on versions |
| Device ID: Is cookie disabled | Checks if cookie is disabled for the user based on history |
| Device ID: Is cookie empty | Checks if cookie value is empty or not empty. Validation check is not included |
| Device ID: Is Cookie from same device | Checks if the HTTP and flash cookies are from same device. Automatically checks old nodes, if current node is not found |
| Device ID: Is Cookie Old | Checks if the cookie sent is from old cookie |
| Device ID: Is cookie valid | Checks if there is a valid node for given cookie value |
| Device ID: known header data match percentage | Checks if known header data match percentage is within specified range |
| Device ID: User ASN for first time | Checks if the user has used this ASN successfully previously |
| Device ID: User used this fingerprint | Checks if the user has used this fingerprint previously |

# C.2  Descriptions

This chapter focuses on device, autolearning, location, transaction, session, system, and user conditions.

The appendix is organized as follows:

- Autolearning Conditions
- Device Conditions
- Session Conditions
- Location Conditions
- System Conditions
- Transactions Conditions
- User Conditions

## C.2.1  Autolearning Conditions

The section provides information on the following autolearning conditions:

- Pattern (Authentication): Entity is Member of Pattern Bucket for First Time in Certain Time Period
- Pattern (Authentication): Entity is Member of Pattern Less Than Some Percent Time
- Pattern (Authentication): Entity is Member of Pattern Less Than Some Percent with All Entities in Picture
- Pattern (Authentication): Entity is Member of Pattern N Times
- Pattern (Authentication): Entity is Member of Pattern N Times in a Given Time Period

### C.2.1.1 Pattern (Authentication): Entity is Member of Pattern Bucket for First Time in Certain Time Period

General information about the condition is provided in the following table.

| Condition | Entity: Entity is Member of Pattern Bucket for First Time in Certain Time Period |
|---|---|
| Description | This condition determine whether this entity is member of a pattern bucket for the first time in a certain time period. First time is a relative function. So if you want to track the first time for the membership, then in rule configuration use "Years" as the "Time period type for bucket membership" and specify a long time such as 5 years or so for the "Time period for bucket membership." This pattern operates on first class entities such as user, device, IP, city, state, and country. |
| Prerequisites | An authentication transaction type pattern has been created with a first class entity member type defined. This pattern operates on first class entities such as user, device, IP, city, state, country. |
| Assumptions | Autolearning is enabled. |
| Available since version | 10.1.4.5 |
| Checkpoints | All checkpoints. |

#### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Pattern Name | Name of the pattern for which the "first time" bucket is to be checked. | | No |
| Is | Evaluate this condition to true if this parameter is true and "first time" bucket is true. | | No |
| Time period type for bucket membership | The time period type (hours, days, months, and years) | One of wotk.type.enum. That is (hour, day, month, year) | No |
| Time period for bucket membership | The time period over which the pattern membership is evaluated. The units of time | Positive integers | No |
| Member type for pattern-bucket membership | The member type (user, device, location, city, country) | Type for members applicable for that transaction. For authentication type it is one of user, device, IP, city, state, country. | No |
| First time count | The count of occurrences to compare against | If you are using this rule in a Pre-Authentication (or pre-transaction) scenario, then use a value of 0 since autolearning takes place on the trailing edge of authentication or transaction. For all other checkpoints, use a value of 1 for this parameter. (1 is also a default value) | No |

#### Example Usage

A pattern and rule could be configured to detect if the current access request is the first time the user has accessed from the state they are in now in the given time frame. For

example, is this the first time in the last six months that John has logged in from California?

### C.2.1.2 Pattern (Authentication): Entity is Member of Pattern Less Than Some Percent Time

General information about the condition is provided in the following table.

| Condition | Entity: Entity is Member of Pattern Less than Some Percent Times |
|---|---|
| Description | Condition determines if the current entity has been a member of the current pattern bucket less than the configured percentage within the time period. |
| Prerequisites | An authentication transaction type pattern has been created with a first class entity member type defined. |
| Assumptions | Autolearning is enabled. |
| Available since version | 10.1.4.5 |
| Checkpoints | All checkpoints. This condition can be used in any checkpoint, but if the data is not processed by then, the data used will be stale by a session. This condition is for the authentication type only. |

#### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Pattern Hit Percent less than | If the current entity behavior has occurred less than the specified percentage the condition should trigger. | Only integer values should be used. | No |
| Pattern name for membership | Name of the pattern this rule condition will evaluate against. | | No |
| Is Membership Count Less than patternHitPercent | This setting controls if the evaluation triggers when it is above or below the specified percentage. | | No |
| Time period type for pattern membership | The time period type (hours, days, months of years) | One of wotk.type.enum. That is (hour, day, month, year) | No |
| Time period for pattern membership | The time window for the pattern membership evaluation. | Positive integers | No |
| Member type for pattern membership | The member type (user, device, location, city, country) | Type of members applicable for that transaction. For authentication type, it is one of user, device, IP, city, state, country. | No |

#### Example Usage

Trigger if this user accessed from the current state they are in less than 3% of the time in the last two months. For example, has John logged in from California less than 5% of the time in the last two months?

### C.2.1.3 Pattern (Authentication): Entity is Member of Pattern Less Than Some Percent with All Entities in Picture

General information about the condition is provided in the following table.

| Condition | Pattern (Authentication): Entity is Member of Pattern Bucket Less Than Some Percent with All Entities in Picture |
|---|---|
| Description | Condition to determine whether the entity is a member of a pattern bucket some percent of time as compared to all other entities that have been member of this pattern. |
| | This condition considers all the other entities; therefore performance is affected more than for simpler conditions. |
| Prerequisites | Entities and patterns must be defined before adding the condition to the rule/policy |
| Assumptions | Autolearning is enabled. |
| Available since version | 10.1.4.5 |
| Checkpoints | Condition can be used in any checkpoint, but if data is not processed by then the data used will be stale by a session. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Pattern bucket hit percent less than | If the current entity behavior has occurred less than the specified percentage the condition should trigger. | Integers. Decimals are not recommended. | No |
| Pattern name for membership | Name of the pattern this rule condition will evaluate against. | | No |
| Is Membership Count Less than patternHitPercent | This setting controls if the evaluation triggers when it is above or below the specified percentage. | | No |
| Time period type for pattern membership | The time period type (hours, days, months of years) | One of wotk.type.enum. That is (hour, day, month, year) | No |
| Time period for pattern membership | Time window for the percentage evaluation. | Positive integers | No |
| Member type for pattern membership | The member type (user, device, location, city, country) | Type of members applicable for that transaction. For authentication type it can be user, device, IP, city, state, or country. | No |

**Example Usage**

Trigger if the current state a user is accessing from is one that other users have utilized a very low percentage of the time within the specified time range. For example, have all users logged in from California less than 5% of the time in the last year?

### C.2.1.4 Pattern (Authentication): Entity is Member of Pattern N Times

General information about the condition is provided in the following table.

| Condition | Pattern (Authentication): Entity is Member of Pattern N Times |
|---|---|
| Description | Condition to determine whether this entity is a member of the pattern more than "n" number of times. This condition is intended to be used only with single bucket type patterns since it evaluates pattern membership as opposed to individual bucket membership. |
| Prerequisites | You should have entities and patterns defined before you try to add this to rule / policy. |
| Assumptions | Autolearning is enabled. |
| Available since version | 10.1.4.5 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Pattern hit count more than | If the current entity behavior has occurred more than the specified count, the condition should trigger. | For Pre-Authentication execution, set the count one less than what you want the rule to trigger on. | No |
| Pattern name for membership | Name of the pattern this rule condition will evaluate against. | | No |
| Is Membership Count More than patternHitCountFor User | Boolean value that is used to return true or false from the condition. It works as follows:<br><br>if (isMoreThan == true) and (hitCountMorethan returned true)<br><br>then condition evaluates to true.<br><br>ELSE if (isMoreThan == false) and (hitCountMorethan returned false)<br><br>then condition evaluates to false. and condition evaluates to false in all other cases. | | No |
| Time period type for pattern membership | The time period type (hours, days, months of years) | One of wotk.type.enum. That is (hour, day, month, year) | No |
| Time period for pattern membership | Time window for bucket membership evaluation. | Positive integers | No |
| Member type for pattern membership | The member type (user, device, location, city, country) | Type of members applicable for that transaction. For authentication type, the type can be user, device, IP, city, state, and country. | No |

**Example Usage**

A single bucket pattern for China is created. Trigger if the current user is coming from China and has accessed from China more than a set number of times within a time range. For example, has John logged in from China more than 4 times in the last six months?

### C.2.1.5 Pattern (Authentication): Entity is Member of Pattern N Times in a Given Time Period

General information about the condition is provided in the following table.

| Condition | Pattern (Authentication): Entity is Member of Pattern N Times in a Given Time Period |
|---|---|
| Description | Condition to determine whether this entity has been a member of the current pattern bucket more than "n" number of times within the given time range. This condition is intended to be used only with both single bucket and multi-bucket type patterns. It evaluates individual bucket membership. |
| Prerequisites | Ensure that the following prerequisites are met:<br>■ 10.1.4.5.2 or later must be installed.<br>■ Entities and patterns must be defined before adding this condition to rules/policies. |
| Assumptions | Autolearning is enabled. |
| Available since version | 10.1.4.5.2 |
| Checkpoints | All checkpoints |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Pattern name for membership | Name of the pattern this rule condition will evaluate against. | | No |
| 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 through 23 for hours. 1 through 30 for days. 1 through 12 for months and 1 through 8 for years. Server will use the use the max values if you enter values more than the above specified. | No |
| 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) | No |
| Member type for pattern 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. | No |
| Bucket hit count | The number of request for the application which will be compared against. Hit count for the bucket and the compare operator used in Pattern (Authentication): Entity is Member of Pattern N Times in a Given Time Period evaluate the outcome of the condition together. | For Pre-authentication execution set the count one less than what you want the rule to trigger on. | No |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Compare operator for the count | Comparison operator to be used for comparing the count in the system with bucketHitCountForEntity. For example if you specified the compare operator as "Less Than" and bucket hit count as 3, the condition will evaluate to true as long as hit count for that bucket is less than 3 for that authentication. | Possible values are 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. | No |
| Return value if condition is true | 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 | No |
| Return value if condition encounters an error | This is the value that will returned if the condition execution runs into issue. Possible errors might be that the pattern is not active, the parameters that were passed (configured) are incorrect or they do not have the values in the expected range. | True / False | No |

### Example Usage

Trigger if the current user has accessed from the current location less than a set number of times within a time range. For example, out of all the states John has logged in from has he come from California less than 4 times in the last month?

## C.2.2 Device Conditions

These section provides information on the following device conditions:

- Device: Browser Header Substring

- Device: Device First Time for User

- Device: Check if Device is of Given Type

- Device: Excessive Use

- Device: In Group

- Device: Is Registered

- Device: Timed Not Status

- Device: Used Count for User

- Device: User Count

- Device: User Status Count

- Device: Velocity from Last Successful Login

### C.2.2.1 Device: Browser Header Substring

General information about the condition is provided in the following table.

| Condition | Device: Browser Header Substring |
|---|---|
| Description | Checks whether the supplied string exists as a substring in the browser's header information. The string comparison is performed by ignoring the case (uppercase or lowercase) of the strings. |
| Prerequisites | |
| Assumptions | The rule is configured through a policy. |
| Available since version | Pre-10.1.4.5 |
| Checkpoints | All checkpoints. |

#### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| subString | Substring to be checked with the string present in the browser. | | Yes |

### C.2.2.2 Device: Check if Device is of Given Type

General information about the condition is provided in the following table.

| Condition | Device: Check if Device is of Given Type |
|---|---|
| Description | Checks whether the current device is of selected device type. It is very helpful to detect mobile or generic devices. |
| Prerequisites | None for condition as such. But you must have rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 11.1.2.0.0 |
| Checkpoints | All checkpoints. |

#### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Device Type | Select Device type to compare with that of current device | Enumeration. Default is Mobile Device<br><br>Other possible value is Desktop Device | No |
| Return value when device is of selected type | Specify the value to be returned if device is of selected type. | Boolean. Default is True.<br><br>True or False | No |

#### Example Usage

Used to check if the device being used is of given type.

To achieve this, you need to use this condition in a rule.

1. Configure the **Devices Type** of this condition as `Mobile Device` and configure the **Return value when device is of selected type** of this condition as `True`.

2. Run authentications from a mobile device, and this rule will trigger.

### C.2.2.3 Device: Device First Time for User

General information about the condition is provided in the following table.

| Condition | Device: Device First Time for User |
|---|---|
| Description | Checks to see if the user is using this device for the first time. Note that "device" is the combination of the physical device and the browser in most of the test scenarios. Check the page of the recent login to determine the Device ID associated with the login sessions to verify the rule. The user's current (session) device is also counted if is found to be used for the first time. |
| Prerequisites | The rule should be configured through a policy. |
| Assumptions | |
| Available since version | Pre-10.1.4.5 |
| Checkpoints | All checkpoints. |

#### Parameters

The following table summarizes the parameters in the condition.

| 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 | No |

#### Example Usage

This condition could potentially be used to determine if the user is logging in from a different device or different devices and to challenge him when it is the case.

### C.2.2.4 Device: Excessive Use

General information about the condition is provided in the following table.

| Condition | Device: Excessive Use |
|---|---|
| Description | Checks to see if this device is used excessively. Basically, checks to see if a device was not active for several days and suddenly a large number of users are logging in from the same device in a short period (in a few hours). This condition can be potentially used to track the compromised device of automated programs that obtained access to the code and then tries to log in several users. |
| Prerequisites | You should have this rule configured through a policy. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All checkpoints. |

#### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| userCount | Number of users logging in from a single device in a short period. | positive integers | No |
| withInHours | This parameter defines the short period in which OAAM must find excessive use. | positive integer | No |
| notInDays | This parameter describes the number of days the device was not in use. | positive integer | No |

**Example Usage**

This condition can be potentially used to determine if the device used in the current activity is compromised. For example, you might have certain devices that are deemed as compromised and you may want to block users logging in from them. For example, an individual could be "hacking" into a bank computer and then trying to perform various activities. Typically, activity logging should be set up for that computer for several days.

### C.2.2.5  Device: In Group

General information about the condition is provided in the following table.

| Condition | Device: In Group |
|---|---|
| Description | Checks to see if the device is in the specified list. |
| Prerequisites | A list defined already which has devices (IDs) as members. |
| | You should have this rule configured through a policy. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| isInList | This is a boolean parameter that defines the 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. OAAM Admin will display a menu with the possible lists of device lists. Use the Group editor in OAAM Admin to edit the device list. | | Yes |

**Example Usage**

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 want to block users logging in from the device that is considered "compromised."

- You may not want users to perform certain activities if they are logging in from a device that is a kiosk.

### C.2.2.6  Device: Is Registered

General information about the condition is provided in the following table.

| Condition | Device: Is Registered |
| --- | --- |
| Description | Condition checks to see if the device where that the user is logging in is registered for the user. |
| Prerequisites Assumptions | You should have this rule configured through a policy. |
| Available since version | 10.1.4.5 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| 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 |

**Example Usage**

This condition can be used to identify if the user is logging in from a device that he has not registered before. This can basically prevent a fraud where the user's login information is stolen and the thief tries to log in using the user's login information from another otherwise safe location.

### C.2.2.7  Device: Timed Not Status

General information about the condition is provided in the following table.

| Condition | Device: Timed Not Status |
| --- | --- |
| Description | This condition counts the attempts by users from the same device (the device used in the attempt) in the last few seconds where the 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. |
| Prerequisites Assumptions | You should have this rule configured through a policy. |
| Available since version | 10.1.4.5 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
| --- | --- | --- | --- |
| status | Count the attempts a status that is not equal to this specified status. | auth.status.enum (auth.status.enum.success is the default) | No |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| withinSeconds | This parameter defines the short period in which the number of login attempts that use that device are counted. | positive integer | No |
| attempts | Maximum number of attempts to watch for. If the attempt count in Oracle Adaptive Access Manager exceeds this number, then the condition will evaluate to true. | positive integer | No |

**Example Usage**

This condition can be potentially used to determine if the device used in the current activity is compromised. A possible fraud scenario can be detected where:

- An individual (or a automated program) uses the same device to make login attempts and the attempts are either failing or passing based on the data that was stolen.

- A program is used to break the password in an automated fashion.

In these cases, there are repeated failed login attempts from the same device in a short amount of time.

### C.2.2.8 Device: Used Count for User

General information about the condition is provided in the following table.

| Condition | Device: Used Count for User |
|---|---|
| Description | This condition counts the attempts by users from the same device (the device used in the attempt) in the last few seconds with an authentication status that is not the one that is specified in the condition. If this count exceeds the count configured in the condition, then this condition evaluates to true. |
| Prerequisites | You should have this rule configured through a policy. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| status | 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 in which login attempts using that device are counted. | positive integer | No |
| attempts | Maximum number of attempts to watch for. If the attempt count exceeds this number then the condition will evaluate to true. | positive integer | No |

**Example Usage**

This condition can be potentially used to determine if the device used in the current activity is compromised.

Possible fraud scenarios that can be detected are:

- An individual (or an automated program) is using same device to make login attempts and the attempts are either failing or passing based on the data that was stolen

- A program is trying to break the password for user in automated fashion

In these cases, repeated failed login attempts are made from the same device in a short period.

### C.2.2.9  Device: User Count

General information about the condition is provided in the following table.

| Condition | Device: User Count |
|---|---|
| Description | Check to see if this device is used by several 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 a number of users. |
| Prerequisites | You should have this rule configured through a policy. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All checkpoints. |

#### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| numberOfUsers | Number of users logging in from the same device in a short period. | positive integers | No |
| withinSeconds | This parameter defines the short period in which the number of users try to log in to the system using that device. | positive integer | No |

#### Example Usage

This condition can be potentially used to determine if the device used in the current activity is compromised. It could be possible that a fraudster had stolen the login information for several users and tried to ruin their accounts. The result is that many users are logging in from the same device in intervals that are a few seconds each.

### C.2.2.10  Device: User Status Count

General information about the condition is provided in the following table.

| Condition | Device: User Status Count |
|---|---|
| Description | Checks user count with the given status from this device in specified duration |
| Prerequisites | None for condition as such. But you must have rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All checkpoints |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
| --- | --- | --- | --- |
| Within | Number of time units to look back in history | Positive Integer. Default = 3 | No |
| Unit of time | Time units to be associated with the within parameter | Integer. time.unit.enum<br><br>Milliseconds, Seconds, Minutes, Hours, Days, Weeks, Months, Years | No |
| Max Users Allowed | Max number of users allowed for this condition to start triggering | Positive Integer. Default = 3 | No |
| With Status | Name of the group that is of type auth status. | Long. ID of the group | Yes |

**Example Usage**

Determine if too many users have logins from the logins that failed from the device in the last three hours.

1. Create a Group of Authentication statuses and add "wrong_password" status to this group.

2. Configure the **Within** parameter to 5.

3. Configure the **Unit of time** to Minutes.

4. Configure the **Max Users Allowed** to 3.

5. Configure the **With Statu**s to the group name that your created above.

Perform logins from this device with the wrong password for four users. The rule triggers for the fifth login. Wait for longer than 5 minutes, and perform the login again; rule will not trigger.

### C.2.2.11  Device: Velocity from Last Successful Login

General information about the condition is provided in the following table.

| Condition | Device: Velocity from Last Successful Login |
| --- | --- |
| Description | Condition evaluates if the user's velocity in miles per hour is more than the specified value. The location database is used to determine the location of the user for this login and previous login. It takes into account the current session as well. Note that the velocity calculation is dependent on the accuracy of the location data. |
| Prerequisites | This rule is configured through a policy. Location database should be loaded for the rule. |
| Assumptions | Location database is loaded. |
| Available since version | 10.1.4.5 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| milesPerHour | Positive number that indicates the user's speed in miles per hour. If the condition determines that the user has traveled faster than this value, then condition will evaluate to `true`. | positive integer (default is 60) | No |
| sinceSeconds | Positive integer that specifies the time difference between this login and last successful login to calculate user's velocity. | positive integer (default is 172800 which is 48 hours) | No |
| Exclude IP List | This parameter allows you to specify a list of IPs to ignore. If a user's IP is from that list, then this condition always evaluates to false. If the user's IP is not in that list or if the list is null or empty, then the condition evaluates the velocity of the user or the device from the last login and evaluates to true if the velocity exceeds the configured value. | | |

### Example Usage

This condition can be used to determine the users' location and the risk it poses because of changes in the user's login location between the time of the current login and the last successful login.

Examples are shown below:

For a case with a user traveling by ground transportation, you can configure this rule so that 60 is the value for miles per hour and the time is in seconds for the last successful login (use default values).

Another case involves users traveling on air transport. You can use different values (for example, 500 miles an hour) to ensure that login locations and speed are within reason.

**Note:** Be aware that the velocity calculation depends highly on location databases.

## C.2.3  Location Conditions

These section provides information on the following location conditions:

- Location: ASN in Group

- Location: in City Group

- Location: In Carrier Group

- Location: In Country Group

- Location: IP Connection Type in Group

- Location: IP in Range Group

- Location: IP Line Speed Type

- Location: IP Maximum Users

- Location: IP Routing Type in Group

- Location: Is IP from AOL

### C.2.3.1  Location: ASN in Group

General information about the condition is provided in the following table.

| Condition | Location: ASN in Group |
| --- | --- |
| Description | Checks 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. |
| Prerequisites | There should a list of ASNs already defined. You should have this rule configured through a policy. |
| Assumptions | |
| Available since version | |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
| --- | --- | --- | --- |
| Is in group | This is a boolean parameter that defines a default return value if the ASN is in the group. | [True] / False | Yes. |
| ASN in ASN group | This is a list of ASN groups. The Rule's Conditions tab will display a menu of possible ASNs groups to for this parameter. Use Group editor in OAAM Admin to edit the ASN group. | | Yes |

**Example Usage**

This condition can be potentially used to determine if the ASN of the current activity (IP) belongs to a particular group of ASNs. For example you might have certain ASNs those can be deemed as dangerous and you may want to block users logging in from there. Or you might not want users to perform certain activity if they are logging in from an ASN that is from a particular country or region.

### C.2.3.2  Location: in City Group

General information about the condition is provided in the following table.

| Condition | Location: in City Group |
| --- | --- |
| Description | Checks whether the current activity belongs to a given city group. |
| Prerequisites | There should a group defined already which has cities as members. You should have this rule configured using a policy. IP location data is useful for this condition. (Most production environments will have IP location database populated) |
| Assumptions | |
| Available since version | |
| Checkpoints | All Checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Is in group | This is a Boolean parameter that defines a default return value if the city is really in country group. | [True] / False | Yes. |
| City in city group | This is a list of city groups. The Rule's Conditions tab displays a drop-down of possible groups of cities. Use Group editor in OAAM Admin Console to edit this group list. | (java Long values) | Yes |

### Example Usage

This condition can be used to figure out if the current activity seems to originate from one of several cities of interest. For example you might have a list of cities and if the current IP of the activity occurs in one of those cities, you can configure the system to take an action or generate an alert.

### C.2.3.3 Location: In Carrier Group

General information about the condition is provided in the following table.

| Condition | Location: Carrier in Group |
|---|---|
| Description | Checks to see if the IP is in the given carrier group |
| Prerequisites | There should a list of carriers already defined. You should have this rule configured using a policy. Location data is helpful for the condition. |
| Assumptions | |
| Available since version | |
| Checkpoints | All checkpoints. |

### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Is in group | This is a Boolean parameter that defines the return value if the carrier is in group or not. | [True] / False | Yes. |
| IP in carrier group | This is a list of the groups of carriers. The Rule's Condition tab displays drop-down of possible lists of carriers groups to configure for this parameter. Use the Group editor in OAAM Admin Console to edit carrier group. | | Yes |

### Example Usage

This condition can be potentially used to check to see if the carrier of the current activity (IP) belongs to a particular list of carriers. For example you might have certain carriers that can be deemed as "dangerous" (hackers stole all of a carrier's phone numbers recently) and you may want to block users logging in from a carrier, or you might not want users to perform a certain activity if they are logging in from a carrier that is from a particular country or region.

### C.2.3.4 Location: In Country Group

General information about the condition is provided in the following table.

| Condition | Location: In Country Group |
|---|---|
| Description | Checks whether the IP belongs to a given country group. |
| Prerequisites | There should a group defined already which has countries as members. You should have this rule configured using a policy. |
| | IP location data is useful for this condition. (Most production environments will have application database populated) |
| Assumptions | |
| Available since version | |
| Checkpoints | All Checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameters | Description | Possible Value | Can be null? |
|---|---|---|---|
| Is in group | This is a boolean parameter that defines a default return value if the country is in country group. | [True] / False | Yes. |
| Country in country group | This is a list of group of countries. The Rule's Condition tab will display a drop-down of possible groups. | (java Long values) | Yes |
| | Use the Group editor in OAAM Admin Console to edit the group. | | |

**Example Usage**

This condition can be potentially used to determine if the current activity seems to originate from one of several countries of interest. For example you might have a list of countries and if the current IP used for the activity belongs to one of those countries, then you can configure the policy to take an action or generate an alert.

### C.2.3.5 Location: IP Connection Type in Group

General information about the condition is provided in the following table.

| Condition | Location: IP Connection Type in Group |
|---|---|
| Description | Determine whether the connection type of this IP location is in the group of connection types that might be of interest. |
| Prerequisites | There should a list of connection types already defined. You should have this rule configured using policies. |
| Assumptions | |
| Available since version | |
| Checkpoints | All Checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Is in group | This is a boolean parameter that defines a default return value if the IP's connection type is really in connection type group. | [True] / False | Yes. |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Connection type in group | This list of connection type groups. The Rule's Condition tab will display a drop-down of possible lists of connection types. Use group editor in administration user interface to edit this group list. | | Yes |

### Example Usage

This condition can be used to determine whether the IP of the current activity comes from a connection type that can be of particular interest to determine fraud. For example, you might have connection type of "satellite link."

### C.2.3.6 Location: IP in Range Group

General information about the condition is provided in the following table.

| Condition | Location: IP in Range Group |
|---|---|
| Description | Checks whether the IP of the current activity belongs to a list of IP-ranges specified. |
| Prerequisites | There should a group defined already which has IP-ranges as members. You should have this rule configured through a policy. |
| Assumptions | |
| Available since version | 10.1.4.5.1 |
| Checkpoints | All checkpoints. |

### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Is IP in IP-range group | Use this parameter to indicate a default return value. If the IP belongs to one of the IP ranges, and this parameter is set to true, condition will evaluate to true. If IP belongs to IP range and the parameter is set to false, the condition will return false | [True] / False | Yes. |
| IP range group | Specify the group that contains the IP ranges. Condition checks if the IP belongs to one of the ranges from this group. | | Yes |

### Example Usage

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 from a particular subnet and you might want to take action if that is the case.

### C.2.3.7 Location: IP Line Speed Type

General information about the condition is provided in the following table.

| Condition | Location: IP Line Speed Type |
|---|---|
| Description | Checks whether the current IP has connection line speed as one of the specified connection speed. This (connection speed) is categorized into High, Medium, Low or Unknown |

| Condition | Location: IP Line Speed Type |
|---|---|
| Prerequisites | You should have this rule configured using a policy. IP location data is useful for this condition. (Most production environments will have IP location database populated) |
| Assumptions | |
| Available since version | |
| Checkpoints | All Checkpoints. |

### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| is | This is a boolean parameter that defines a default return value if the connection speed is the one specified. | [True] / False | Yes. |
| speed type | This is the enumeration value that indicates connection speed type. This (connection speed) is categorized into High, Medium, Low or Unknown<br><br>The enum that is used for this parameter is location.linespeed.enum | (Integer) Default value is location.linespeed.enum.low | Yes |

### Example Usage

This condition can be used potentially to determine whether the current activity seems to originate from an IP that has a particular speed type. For example, you may want an alert generated if the speed type is high for the user who usually logs in from a dial-up network.

### C.2.3.8  Location: IP Maximum Users

General information about the condition is provided in the following table.

| Condition | Location: IP Maximum Users |
|---|---|
| Description | Condition checks to see if the maximum number of distinct users using the current IP address within the given time duration exceeds the configured condition attribute value. Notice that the current request is also counted in finding the number of unique users from the IP. |
| Prerequisites | You should have this rule configured using a policy. |
| Assumptions | |
| Available since version | |
| Checkpoints | All Checkpoints. |

### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Seconds elapsed | This is the time period in which the number of users from this IP is to be counted. | integer [Default is 300] | No |
| The maximum number of users | Maximum number of users allowed. | integer [Default is 5] | No |

**Example Usage**

Use this condition to determine if a particular IP is used by fraudsters to perform logins / transactions by using different login IDs they have stolen. In such cases you see a number of different logins from the same IP during a relatively short period.

### C.2.3.9  Location: IP Routing Type in Group

General information about the condition is provided in the following table.

| Condition | Location: IP Routing Type in Group |
|---|---|
| Description | Checks to see if the IP Routing Type is in the group. |
| Prerequisites | There should a group defined already which has routing types as members. You should have this rule configured using a policy. IP location data is useful for this condition. (Most production environments will have IP location database populated) |
| Assumptions | |
| Available since version | |
| Checkpoints | All Checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Is in group | This is a boolean parameter that defines a default return value if the IP routing type is in group. | [True] / False | Yes. |
| Routing type in group | This is a list of groups of IP routing types. A drop-down of possible lists of IP routing type groups. Use the Group editor in OAAM Admin to edit this group list. | (java Long values) | Yes |

**Example Usage**

This condition can be potentially used to determine whether the current activity is from an IP that belongs to a particular routing type. For example, you might have a list of routing types that can potentially lead to fraud and if the current IP of the activity has one of those routing types, you can configure to take an action or generate an alert.

### C.2.3.10  Location: Is IP from AOL

General information about the condition is provided in the following table.

| Condition | Location: Is IP from AOL |
|---|---|
| Description | Determine whether the IP is from AOL proxy |
| Prerequisites | You should have this rule configured using a policy to test it. |
| Assumptions | |
| Available since version | |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|-----------|-------------|-----------------|--------------|
| Is AOL | This is the default return value is IP is indeed from AOL. If the IP is not from AOL then opposite of this attribute is returned. | Boolean [true] / false | No |

**Example Usage**

This condition can be used to figure out if the IP is from an AOL proxy. Customers may want to set up the system to take certain actions for users logging in from AOL.

## C.2.4 Session Conditions

The following Session conditions are documented in this section:

- Session: Check Param Value

- Session: Check Param Value in Group

- Session: Check Param Value for Regex

- Session: Check two string param value

- Session: Check String Value

- Session: Time Unit Condition

- Session: Compare Two Parameter Values

- Session: Check Current Session Using the Filter Conditions

- Session: Check Risk Score Classification

- Session: Cookie Mismatch

- Session: Mismatch in Browser Fingerprint

- Session: Compare with Current Date Time

- Session: IP Changed

- Session: Check value in comma separated values

### C.2.4.1 Session: Check Param Value

General information about the condition is provided in the following table.

| Condition | Session: Check Param Value |
|-----------|----------------------------|
| Description | Check to see whether the specified parameter value is above the given threshold. This condition can be used to determine whether the value of a particular parameter in the transaction is above some known threshold and then action can be taken accordingly. Basically provided a mathematical function for integrators. This will be very useful in native integration. |
| Prerequisites | None for condition as such. But you must have rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Checkpoints. |

**C.2.4.1.1  Parameters**  The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|-----------|-------------|-----------------|--------------|
| Is | If the "Is" is true and the value is above the threshold provided then condition evaluates to true.<br><br>If the "Is" is false and the value is below the threshold provided then condition evaluates to true. | [True] / False | No |
| ValueKey | The "key" or the look up name of the parameter in the transaction. For example if the transaction is purchase and the name of the attribute is "creditcard" and whose value at Checkpoint is going to be populated by users credit card, then key is "creditcard" in this case. If key is null then defaultError return value is the result of the condition. | | Yes |
| ValueAbove | This is basically the threshold value. This can be used to see if the time is greater than the time parameter present in the transaction. It accepts string representations of long values. Note: If you want to create a rule that uses a decimal value, use the condition Session: Check string param value. | Long values | Yes |

**C.2.4.1.2  Example Usage**  Use this condition when you want to determine whether the value of a particular attribute of the transaction exceeds some threshold.

For example, you configured a transaction called purchase want to trigger a rule whenever the customer purchase exceeds $1000 Mark.

For accomplish this, you must use this rule with this condition.

1. Configure the "ValueKey" of your transaction to "purchase.orderTotal" assuming that you have such an attribute in your transaction.

2. Configure "ValueAbove" to "1000". Configure an alert that says "Too Big Purchase."

3. Process a transaction by providing a few total value numbers above 1000 and a few below 1000.

4. Verify that for the ones above 1000 the rule is triggered.

### C.2.4.2  Session: Check Param Value in Group

General information about the condition is provided in the following table.

| Condition | Session: Check Param Value in Group |
|-----------|-------------------------------------|
| Description | Checks to see if specified parameter value matches the regular expression and the group identified by the expression matcher is in the list of strings. Regular expression matching is not sensitive to case (uppercase and lowercase letters are treated same) |
| Prerequisites | None for condition as such, but you must have a rule configured with this condition for it to work. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Value | Can be Null |
|---|---|---|---|
| Is | If the "Is" is true and the key's value matches the regular expression and the first group string found by the regex matcher is in the string group, then the condition evaluates to "true." | [True] / False | Yes |
| Parameter Key | The "key" or the look up name of the parameter in the transaction. For example, if the transaction is "internet banking" and the name of the attribute is "bankName" and its value at checkpoint is to be populated by users, then key is "Transaction.bankName" in this case. You should be able to find this key in the Internal ID column in the Transaction Source Data tab in transaction details. If the key is null, then defaultReturnValue is the result of the condition. | | Yes |
| Regular Expression | The character pattern with which you want to match the "value" which has its look up name given by "Parameter Key". In same banking example, if you want to determine whether the bankName equals "SomeBank," you should define this pattern in the policy/rule as "(SomeBank)" without the quotation marks. If the regular expression is null, then defaultReturnValue is the result of the condition. | | Yes |
| In list | The condition checks to see if the character group obtained by the regular expression matcher belongs to this string group. If the list name is null or if the list specified by the name is empty, then defaultReturnValue is the result of the condition. | | Yes |
| Default Return value | If there is any error or if the condition cannot be evaluated because of insufficient data, then return (evaluate to) this value. If this value is not specified (null) then "False" is assumed. | [False] / True | Yes |

**Example Usage**

Use this condition when you want to determine whether some part of the value of a particular attribute of the transaction matches some character pattern, and to see if this part of the value is present in the pre-determined group of strings.

For example, you have configured a transaction called internet banking and you want to trigger a rule if the bank name is "bank1" or "bank2."

To achieve this, you must use this rule with this condition:

1. Configure the "Parameter Key" of your transaction to "Transaction.bankName" (assuming that you have such an attribute in your transaction).

2. Configure "Regular Expression" to "(bank.)". Configure an alert that says "Some specified bank transaction".

3. Create a group of generic strings called "interesting banks" and add "bank1" and "bank2" to it.

4. Configure the group name as "In List" parameter for this condition.

5. Configure "Is" to true and default return value to false.

6. Process a few transaction by providing bank names, "bank1" and "bank2","bank3", and so on. Verify that the alert is generated for "bank1" and "bank2" only.

7. Verify that alerts are generated for "BANK1". This shows that the regular expression matching is not case-sensitive.

### C.2.4.3 Session: Check Param Value for Regex

General information about the condition is provided in the following table.

| Condition | Session: Check Param Value for Regex |
|---|---|
| Description | Determine whether the specified parameter value matches regular expression. This condition can be used to determine whether a string value of a particular parameter in the transaction matches a known pattern and then action can be taken accordingly. This provided a mathematical function for integrators and is useful in native integration. |
| Prerequisites | None for condition as such. But you must have rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Checkpoints. |

**C.2.4.3.1 Parameters** The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Is | If the "Is" is true and regular expression matches to the provided criteria then condition evaluates to true.<br><br>If the "Is" is false and regular expression does not match to the provided criteria then condition evaluates to true. | [True] / False | No |
| ValueKey | The "key" or the look up name of the parameter in the transaction. For example if the transaction is purchase and the name of the attribute is "creditcard" and whose value at Checkpoint is going to be populated by users credit card, then key is "creditcard" in this case. If key is null then defaultError return value is the result of the condition. You should be able to find this key in the Internal ID column in Transaction Source Data tab in transaction details. | | Yes |
| Regular Expression | The character pattern with which you want to match the "value" whose look up name is given by "ValueKey". In same credit card example. Check to see whether the user entered all correct in credit card so you might look for pattern "[0-9]". | | Yes |
| Error Return value | If there is any error then return (evaluate to) this value. If this value is not specified (null) then "False" is assumed. | [False] / True | Yes |

**C.2.4.3.2 Example Usage** Use this condition to determine whether the value of a particular attribute of the transaction matches some character pattern.

For example, you configured a transaction called "purchase" and want to trigger a rule whenever the customer email field ends with ".gov" or ".mil" so you can track government and military business for your firm.

For accomplish this, you must use this rule with this condition.

1. Configure the "ValueKey" of your transaction to "customer.email" assuming that you have such a attribute in your transaction.

2. Configure "Regular Expression" to "*[.gov][.mil]".

3. Configure an alert that says "Government/Military business."

4. Process a few transaction by providing email addresses ending with ".gov" or ".mil".

5. Verify that the alert is generated.

6. Process a few transactions by giving another email address ending with ".com" or any ending other than ".gov" or ".mil".

   Notice that alert is not generated.

### C.2.4.4  Session: Check two string param value

General information about the condition is provided in the following table.

| Condition | Session: Check two string param value |
| --- | --- |
| Description | Check to see whether the specified parameter value is equal to a given character string. This condition can be used to determine whether the value of a particular parameter in the transaction matches an expected string so that action can be taken accordingly. Basically the condition provided a string equality function for integrators. This is useful in native integration. |
| | Note that the comparison is case-sensitive. That is "Good" is not equal to "GOOD". |
| Prerequisites | None for condition as such, but you must configure a rule with this condition for the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
| --- | --- | --- | --- |
| ValueKey | The "key" or the look up name of the parameter in the transaction. For example if the transaction is purchase and the name of the attribute is "creditCardType" and whose value at Checkpoint is going to be populated by users credit card type, then key is "creditCardType" in this case. | | Yes |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| StringValue | This is basically the value to compare with. | | Yes |

### Example Usage

Use this condition when you want to determine whether the value of a particular attribute of the transaction equals a given string.

For example, you have configured a transaction called purchase and you want to trigger a rule whenever the customer credit card is American Express.

To accomplish this, you must use this rule with this condition:

1. Configure the "ValueKey" of your transaction to "purchase.creditCardType" assuming that you have such an attribute in your transaction.

2. Configure "StrValue" to "AMEX". Configure an alert that says "Amex Card Used"

3. Process a few transactions by providing the card type as AMEX and a few with another card type.

4. Verify that when AMEX is used, the rule is triggered.

### C.2.4.5  Session: Check String Value

General information about the condition is provided in the following table.

| Condition | Session: Check String Value |
|---|---|
| Description | Check to see whether the specified parameter value is equal to a given character string. This condition can be used to determine whether the value of a particular parameter in the transaction matches an expected string so that action can be taken accordingly. Basically the condition provided a string equality function for integrators. This is useful in native integration. |
| | Note that the comparison is case-sensitive. That is "Good" is not equal to "GOOD". |
| Prerequisites | None for condition as such, but you must configure a rule with this condition for the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Checkpoints. |

**C.2.4.5.1  Parameters**  The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Value | Can be Null? |
|---|---|---|---|
| ValueKey | The "key" or the look up name of the parameter in the transaction. For example if the transaction is purchase and the name of the attribute is "creditCardType" and whose value at Checkpoint is going to be populated by users credit card type, then key is "creditCardType" in this case. | | Yes |
| StringValue | This is basically the value to compare with. | | Yes |

**C.2.4.5.2  Example Usage**  Use this condition when you want to determine whether the value of a particular attribute of the transaction equals a given string.

For example, you have configured a transaction called purchase and you want to trigger a rule whenever the customer credit card is American Express.

To accomplish this, you must use this rule with this condition:

1. Configure the "ValueKey" of your transaction to "purchase.creditCardType" assuming that you have such an attribute in your transaction.

2. Configure "StrValue" to "AMEX". Configure an alert that says "Amex Card Used"

3. Process a few transactions by providing the card type as AMEX and a few with another card type.

4. Verify that when AMEX is used, the rule is triggered.

### C.2.4.6 Session: Time Unit Condition

General information about the condition is provided in the following table.

*Table C–3 Day of Week*

| Condition | Day of Week |
|---|---|
| Description | Checks to see if time unit in current date matches certain criteria. The condition determines if a particular time unit (that is part of the current time) belongs to a particular position in the time unit. |
| | This condition uses the request date if available to evaluate the date function requested with the help of parameters. |
| | If the request date is not available, then current server date time will be used. |
| Example | This condition can determine if the day of the week is equal to (or not equal to or …) Monday or Tuesday and so on. |
| | It can also determine if the day of the month matches certain criteria of the day of the month. |
| | It can also try to match the same criteria if month of the year is X or not X or in or not in X. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameters | Description | Possible Values |
|---|---|---|
| Time Unit | Enum | Possible values are: |
| | What is the time unit you are looking for? | ■ Day Of the Week |
| | The default value is Day Of The Week | ■ Day Of the Month |
| | | ■ Day of the year |
| | | ■ Month of the Year |
| | | ■ Hour of the day |
| | | ■ Week Of the Month |
| | | ■ Week Of The year |
| | | ■ Year |
| Comparison operator | Enum | Possible values are: |
| | What comparison you want to make with the time unit. | ■ Equal To |
| | The default value is Equal To | ■ Not Equal To |
| | | ■ Less than |
| | | ■ More Than |
| | | ■ Less than equal to |
| | | ■ more than equal to |
| | | ■ IN |
| | | ■ not IN |

| Parameters | Description | Possible Values |
|---|---|---|
| Comparison value | String<br><br>The default value is "" (empty string), that represents integer or string that represents comma separated integers. Example: "1" or "1,2,3,4".<br><br>The user can use comma-separated values when using IN or NOT in operator.<br><br>If comma-separated values are used for any other operators, it will be determined as an error and value of the number 5 parameter (shown in Error Return) will be returned.<br><br>If the string does not represent number (or a list of comma separated numbers) then it is determined as error and value of parameter number 5 will be returned. | Correct values of this parameter for different time units.<br><br>■ Day Of The week: 1 through 7 (1 is Sunday).<br><br>■ Day Of the month: 1 through 31<br><br>■ Day of the year: 1 through 366<br><br>■ Month of the year: 0 through 11 (0 is January)<br><br>■ Hour of the day: 0 through 23<br><br>■ Week of the Month: 0 through 6<br><br>■ Week of the Year 1 through 53<br><br>■ Year: Positive integer |
| IS Condition True | Boolean<br><br>Default value is true<br><br>This will the return value if the comparison is true. | |
| Error Return value | Boolean<br><br>Default value is false<br><br>If the user has configured the value of Comparison Value (#3) incorrectly, or if there is any other error determining date then this value will be returned.<br><br>The days of the weeks are:<br><br>■ 1 = sunday<br><br>■ 2 = monday<br><br>■ 3 = tuesday<br><br>■ 4 = wednesday<br><br>■ 5 = thursday<br><br>■ 6 = friday<br><br>■ 7 = saturday<br><br>The week day is 2,3,4,5,6<br><br>Time Unit is Day of the Week<br><br>Comparison Operator is "IN"<br><br>Comparison Value is "1,2,3,4,5"<br><br>Is Condition True is true<br><br>Error Return value is "false" | |

## C.2.4.7  Session: Compare Two Parameter Values

General information about the condition is provided in the following table.

| Condition | Session: Compare Two Parameter Values |
|---|---|
| Description | Compares the specified parameter values based on the compare operator, and if based on flag if case (upper / lower) should be used for string type parameters. This condition can be used to check if value of a particular parameter in the transaction is above / below / equal to some other parameter. Basically provided some mathematical function for integrators. Before doing the compare the values of the actual items in the transaction are converted to string (characters) for comparison. |
| Prerequisites | None for the condition as such, but you must have the rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All runtimes |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Parameter Key1 | The "key" or the look up name of the parameter in the transaction. For example if the transaction is purchase and the name of the attribute is "shippingaddresszip" and whose value at runtime is going to be populated by users shipping address zip code, then key is "shippingaddresszip" in this case. If key is null then defRetValue return value is the result of the condition. | String | No |
| Parameter Key2 | The "key" or the look up name of the parameter in the transaction. For example if the transaction is purchase and the name of the attribute is "billingaddresszip" and whose value at runtime is going to be populated by users billing address zip code, then key is "billingaddresszip" in this case. If key is null then defRetValue return value is the result of the condition. | String | No |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Operation | This is the compare operation to be used on the values associated with two keys above. This operator is used as result = (value1) [This compare operation] (value2)<br><br>For example if value1 = numeric amount1 (say = 100.00 Dollars) and value2 = numeric amount2 (say = 53.23 dollars) and this operator is say "more than" then the condition evaluates to<br><br>100.00 [ More than] 53.23 === False. | =, <, >, <=, >=, <>, contains, starts with, ends with | Yes |
| IgnoreCase | Whether case (upper case / lower case) should be ignored for string representations of the parameters. | [True] / False | No |
| Default Return Value | Default value of the condition if there is any error in getting the params or if one of both of the params cannot be found, or are empty or null. | [False] / True | No |

**Example Usage**

Use this condition whenever you want to compare the values of two attributes of the transaction. For example, you have configured a transaction called purchase and you want to trigger a rule whenever the customer's billing zip code and shipping zip code are not same. For achieving this, you need to use this rule with this condition.

1. Configure the **Parameter Key1** of your transaction as **purchase.billingZipCode**. This assumes that you have such a attribute in your transaction.

2. Configure the **Parameter Key2** of your transaction as **purchase.shippingZipCode**. This assumes that you have such a attribute in your transaction.

3. Configure **compareOperator** as **not equals**. Configure an alert that says "Billing and Shipping Code no match."

4. Process a transaction by providing different billing and shipping zip codes.

5. Verify that the rule is triggers. Also verify that if the transaction has the same billing and shipping zip code, the rule does not trigger.

### C.2.4.8  Session: Check Current Session Using the Filter Conditions

General information about the condition is provided in the following table.

| Condition | Session: Check Current Session Using the Filter Conditions |
|---|---|
| Description | Compares the attributes of the session with the specified value of the current value. This condition can use up to six filter condition which are logical "AND"ed to get the final result of the condition. |
| | This condition lets you build a expression. You can build expression that have the attributes of session also available. Expression building can be viewed as |
| | Expr1 = right side variable <Operator> left side variable or Value |
| | AND |
| | Expr2 = right side variable <Operator> left aide variable or Value |
| | .... and so on. |
| | You can add up to 6 expressions to build your logic. |
| | The variables available are the attributes of the session that are available in the environment when this condition is evaluated. |
| Prerequisites | None for condition as such, but you must have rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 11.1.2.0.0 |
| Checkpoints | All Checkpoints except Device ID. |

### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Check If (or the right side of the expression) | The attribute of the session to be compared. This should be selected from pre-determined list of attributes that are available. It is required to have at least one attribute (row) in the condition. | Drop_Down | No |
| Operator | Select the appropriate operator from the list of available operators. | Drop Down, select one of <br> <, >, <=, >=, =, Not Equal to, Equals Ignore case, is null, is not null, in, not in, like, not like | No |
| Value / Current | Choose the value if you want to specify absolute value or current if you want to compare with the current other attribute of the session. | Value / Current | No |
| Right side of value | If you selected the value in the value/current, you will be provided with the text box to enter the absolute value to be used as right side of expression. <br><br> If you chose Current in the previous box, then you will get a drop down of the available attributes to compare. | String Value | Yes |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| and | You can repeat the rows of left side : operator: right side to build your expression. | | |

**Example Usage**

This condition can be used whenever you want to compare the values of the session and build a chain of expressions and build your own logic

For example, if you want to see if the IP Address of the session is not localhost and users are logging in from Mozilla type browsers. For achieving this, you need to this condition in a rule.

1. Configure on the first expression, "Check If" "IP Address" "Not Equals" "Value" and type in "127.0.0.1" in the box

2. On the second line of expression configure, "AND" "Session.Browser.UserAgent" "Like" "Value" and then type in "Mozilla".

3. Perform logins from an IP Address other than 127.0.0.1 with Mozilla browser, the rule should trigger.

4. Do some logins from same IP Address with other browser say Internet Explorer of Safari or such, the should not trigger.

### C.2.4.9 Session: Check Risk Score Classification

General information about the condition is provided in the following table.

| Condition | Session: Check Risk Score Classification |
|---|---|
| Description | Checks the risk score classification based on the risk score from previous checkpoint execution |
| Prerequisites | None for condition as such, but you must have rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 11.1.2.0.0 |
| Checkpoints | All Runtimes. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Classification Type | Type or Range of riskscore. Out of box risk score classified in three types or ranges. (low = 0 to 0, medium = 1 to 500, high = 501 to 1000). | (Integer = 0,1,2) Select from Drop down [0=low], 1=medium, 2=high | No |
| Default Return Value | Default value of the condition if there is any error. | [False] / True | No |

**Example Usage**

This condition can be used whenever you want to see if the risk score was in pre-determined range in the previous checkpoints for the same session.

For example, if you want to see if the risk score was in high range in any previous checkpoint in this session. The assumption here is you have only 2 checkpoints here namely pre-authentication and post authentication that have policies in them.

For achieving this, you need to use this rule with this condition.

1. Configure the "risk score type" of your condition as "high."

2. Configure "default return value" as "false".

3. Configure this rule in the post authentication checkpoint.

4. In Pre-authentication checkpoint configure a rule that emits a high score. (It can be done by creating the rule in that checkpoint by adding the "always on" condition to it.)

5. Verify that the rule is triggers.

### C.2.4.10  Session: Cookie Mismatch

General information about the condition is provided in the following table.

| Condition | Session: Cookie Mismatch |
|---|---|
| Description | Checks to see if there is mismatch of supplied cookie with the expected cookie. |
| Prerequisites | None |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Runtimes except Device ID. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Fingerprint Type | Fingerprint type enum for the cookie. Valid values will be browser or flash. | [Browser] or Flash | No |
| CookieKey | Context data key for the cookie value. | String [browser_securecookie] or any String | No |
| Trigger If Match | If set to true, the condition will evaluate to true if the cookies match. | [True] / False | Yes |

**Example Usage**

This condition can be used whenever you want to check if the expected cookie and the actual cookie coming in from this device matches or not.

To use this condition, add it to a rule and use it in say post authentication checkpoint.

You will need to use a simulator or browser modifier extensions to send another cookie instead of the expected one.

1. Add this condition with default values to the rule.

2. Perform logins to make sure that your logins are from the same device--view the Device ID field in the session data.

3. Now use the browser modifier extension or simulator to send a different cookie than expected one.

This rule should trigger.

### C.2.4.11 Session: Mismatch in Browser Fingerprint

General information about the condition is provided in the following table.

| Condition | Session: Mismatch in Browser Fingerprint |
|---|---|
| Description | Checks to see if there is mismatch in browser fingerprint with the fingerprint supplied during authentication. Fingerprint is constructed using the context values passed to Rules Engine. |
| Prerequisites Assumptions | None |
| Available since version | 10.1.4.5 |
| Checkpoints | All Runtimes except Device ID. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| User Agent Key | Context data key for browser user agent value. | String [browser_uas] or any String | No |
| Local Language Key | Key to Local Lang value | String[browser_localLang] or any String | Yes |
| Local Country Key | Key to Local Country value | String[browser_localCountry] or any String | Yes |
| localVariantKey | Key to Local Country value | String[browser_localVariant] or any String | Yes |
| Trigger If Match | If Set (to true), condition is triggered when fingerprints match | [True] / False | Yes |

**Example Usage**

This condition can be used whenever you want to check if the browser fingerprint matches the actual one logging in from the browser for this session.

To use this condition, add it to a rule and use it in the post authentication checkpoint.

You will need to use simulator or browser modifier extensions to send the desired user agent strings.

Add this condition with default values to the rule.

Perform some logins to make sure that your logins are coming in from the same device. View the Device ID field in the session data.

Use the browser modifier extension or simulator to send a different fingerprint than expected one.

The rule should trigger.

### C.2.4.12 Session: Compare with Current Date Time

General information about the condition is provided in the following table.

| Condition | Session: Compare with current date time |
|---|---|
| Description | Compare specified parameter value with current time |
| Prerequisites | None for condition as such, but you must have a rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Runtimes. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Parameter Key | The "key" or the look up name of the parameter in the transaction. For example if the transaction is purchase and the name of the attribute is "po_time" and whose value at runtime is going to be populated by date-time type data., then key is "po_time" in this case. If key is null then condition evaluates to false. If key returns a null date object then "IfNull" return value is the result of the condition. | String | Yes |
| Is after current date? | This is the boolean parameter to configure if the date field should be checked for condition after the current date or before (or equal to) the current date. | Boolean [True]/ False | Yes |
| If given date key returns empty date (ifNull) | This boolean parameter specifies what to do if the Parameter Key did not return a valid date object from transaction data. | Boolean [True]/ False | Yes |

**Example Usage**

This condition can be used whenever you want to compare the value of the date attribute in a transaction with the transaction date itself.

For example, if you have configured a transaction called "Purchase" and you want to trigger a rule whenever the purchase order date is after the current time.

To achieve this, you need to use this rule with this condition.

Configure the "Parameter Key" of your transaction to "purchase.po_date" assuming that you have such a attribute in your transaction.

Configure the "Is after current date" of your transaction to true.

Configure "If given date key returns empty" to false

Process a few transaction by providing different po_date values.

Verify that the rule is triggers when "po_date" is after the current date.

### C.2.4.13  Session: IP Changed

General information about the condition is provided in the following table.

| Condition | Session: IP Changed |
| --- | --- |
| Description | IP Address is changed since transaction is started |
| Prerequisites | None for condition as such, but you must have a rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Runtimes |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
| --- | --- | --- | --- |
| IP Key | The "key" or the look up the IP value in the transaction data. | String | Yes |

**Example Usage**

This condition can be used mostly in transaction related scenarios to compare the value of the IP attribute in a transaction with the current IP address of the session.

For example, if you have configured a transaction called purchase and you want to trigger a rule whenever the IP address coming in the transaction does not match the one that the session is coming from.

To achieve this, you need to use this rule with this condition.

Configure the "IPKey" of your transaction as "purchase.ip_addr" assuming that you have such a attribute in your transaction.

Process a few transaction by providing different ip_addr values.

Verify that the rule is triggers when ip_addr is not the same as the session's IP address.

### C.2.4.14  Session: Check value in comma separated values

General information about the condition is provided in the following table.

| Condition | Session: Check value in comma separated values |
| --- | --- |
| Description | Checks if specified value is present in comma separated value list. Here the comma separated values is the set of values in the transaction data associated with the specified key. |

| Condition | Session: Check value in comma separated values |
|---|---|
| Prerequisites | None for condition as such, but you must have rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Runtimes |

### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Value Key | The "key" or the look up the value in the transaction data.<br><br>The value associated with this key may be comma separated. | String | Yes |
| Value to Check | Value check against | String | Yes |
| IsTrue | Condition evaluates to this value if the value of the key is in list | Boolean | True |

### Example Usage

This condition can be used mostly in transaction related scenarios to compare if one of the data values associated with specified key is the one we are interested in.

For example, you want to identify if the merchant is interested in knowing if the user has stayed in a specified country as part of evaluating the credit card application that is coming in. The countries information comes in as a comma-separated list of strings with country codes. For example: US, UK, and so on.

You configure your transaction as credit_card_application which has a data field that says counties_resided_last_3_years.

Add this condition to the rule that will be executed.

Configure the "ValueKey" of your transaction as "counties_resided_last_3_years"

Configure Value to Check as "US."

Configure isTrue as "True"

Process / perform a few transactions with various combinations of countries resided.

When your comma-separated list of countries resided contains "US" the rule will trigger.

## C.2.5 System Conditions

The following transaction conditions are documented in this section:

- System - Check Boolean Property
- System - Check Enough Pattern Data

- System - Check If Enough Data is Available for Any Pattern

- System - Check Int Property

- System - Check Request Date

- System - Check String Property

### C.2.5.1 System - Check Boolean Property

General information about the condition is provided in the following table.

| Condition | System - Check Boolean Property |
|---|---|
| Description | Verify if specified property equals true of false. |
| Prerequisites | None for condition as such. But you must have rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Checkpoints. |

**C.2.5.1.1  Parameters** The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Value | Can be Null? |
|---|---|---|---|
| Property | The complete name of the property that must be checked. | | Yes |
| PropertyValue | The expected value of the property. If the property has this value then the condition will evaluate to true. | [True] / false | Yes |
| Defaultvalue | The value of the property to be used if the property is not found in the system. | [True] / false | Yes |

**C.2.5.1.2  Example Usage** Use this condition when you want to determine whether the value of a particular property is true or false.

For example, you have a property "trigger.sample.rule" and its value is true.

You want to trigger some rule based on this property.

For accomplish this, you must use this rule with this condition.

1. Configure the "Property" of this condition to "trigger.sample.rule".

2. Configure the PropertyValue to "true".

3. Configure DefaultValue to "false"

4. Run authentication of users to see if the rule triggers.

5. Use the property editor to change the value of the property "trigger.sample.rule" to false.

6. Run authentication of users again and notice that the rule does not trigger.

### C.2.5.2 System - Check Enough Pattern Data

General information about the condition is provided in the following table.

*Table C–4     System - Check enough pattern data*

| Details | Description |
| --- | --- |
| Condition | System - Check enough pattern data |
| Description | Checks if enough profiling data is available for a given pattern. This condition checks if pattern data is available in the system for the last several days. |
| | It checks only for a particular pattern. So if data is available that is collected by the given pattern for more than the specified number of days, this condition evaluates to true. |
| Prerequisites | None for condition as such. But you must have a rule configured with this condition to experience the behavior. |
| Available since version | 11.1.2.0 |
| RunTimes | All Runtimes. |

### Parameters

The following table summarizes the parameters in the condition.

*Table C–5     System - Check enough pattern data parameters*

| Parameter | Description | Possible Values | Can be null? |
| --- | --- | --- | --- |
| patternGlobalIdCheckData | Name of the pattern for which the data availability is to be checked. | Pattern names from drop down list | No |
| numDaysOfDataToCheck | How many days should the condition "look back" from the current login's request time. Typical value is 90 (days). | Positive integer | No |
| | The condition checks these many number of days of data. If pattern profiling data is available for at least these number of days, the condition evaluates to true | | |
| isPatternDataAvailableDataCheck | Condition evaluates to true if this value is true and there is enough autolearning data OR if this value is false and there is not enough autolearning data. In all other cases, the condition evaluates to false. This parameter basically can be used to decide the outcome of the condition. | [True] / False | Yes |
| errorReturnValueDataCheck | Value to return if the condition runs into an error. | [False] / True | Yes |

### Example Usage

Use this condition to check if enough autolearning data exists in the system that had been collected by a given pattern.

"Enough data" can be termed as data gathered over the last several days, depending on the customer scenarios.

For example, this condition can determine if the given autolearning pattern has gathered the data for the last 90 days and based on that, the autolearning rules are used.

The condition provides time for autolearning data to reach statistical stability. If autolearning rules work on a very small set of data, the results may be skewed, depending on how small data sample is.

For example, on a system that just had the pattern enabled today, a customer may want the OAAM Server to gather pattern data for three months before starting testing.

In that case, this condition is useful because it will evaluate to true only after three months (90 days). Then, autolearning rules can trigger and evaluate the risk.

### C.2.5.3  System - Check If Enough Data is Available for Any Pattern

General information about the condition is provided in the following table.

*Table C–6    System - Check If Enough Data is Available for Any Pattern*

| Details | Description |
| --- | --- |
| Condition | System - Check If Enough Data is Available for Any Pattern |
| Description | This condition will check if a defined minimum amount of pattern data has been captured int he OAAM database. Generally the threshold should be set to between 1-3 months for best results. The out of the box policies utilize this rule to determine if there is enough pattern data captured to start running pattern based risk analysis. |
| Prerequisites | None for condition as such, a rule must be configured with this condition to experience the behavior. |
| Assumptions | Autoleaning is enabled. Without active patterns collecting profiling data, this conditions will not be meaningful. |
| Available since version | 11.1.1.5.0 |
| RunTimes | All Runtimes. |

**Parameters**

The following table summarizes the parameters in the condition.

*Table C–7   System - Check If Enough Data is Available for Any Pattern Parameters*

| Parameter | Description | Possible Value | Can be Null? |
|---|---|---|---|
| numDaysOfDataToCheckAnyPattern | How many days should condition "look back" from the current login's request time. Typical value is 90 (days). | Positive integer | No |
| | Condition checks these many number of days of data. If pattern profiling data is available for at least these number of days, the condition will evaluate to true. | | |
| isPatternDataAvailableDataCheckAnyPattern | Condition evaluates to true if this value is true and there is enough autolearning data OR if this value is false and there is not enough autolearning data. In all other cases, the condition evaluates to false. This parameter can be used to decide the outcome of the condition. | [True] / False | Yes |
| errorReturnValueDataCheckAnyPattern | Value to return if the condition runs into an error. | [False] / True | Yes |

**Possible Scenarios**

Use this condition to check if enough autolearning data exists in the system.

"Enough data" can be termed as data gathered over the last several days depending on the customer scenarios.

This condition can determine if any of the autolearning pattern have gathered data for the last 90 days, and based on that, auto learning rules can be used.

This provides time for autolearning data to reach statistical stability. Otherwise, if autolearning rules work on a very small set of data, the results may be skewed depending on how small the data sample is.

For example: on a system that has patterns enabled today, customers may want OAAM Server to gather pattern data for three months before starting to use autolearning rules. In that case, this condition is useful. It evaluates to true only after three months (90 days) and then autolearning rules can trigger and evaluate the risk.

### C.2.5.4  System - Check Int Property

General information about the condition is provided in the following table.

| Condition | System - Check Integer Property |
|---|---|
| Description | Verify if specified property equals expected integer value |
| Prerequisites | None for condition as such. But you must have rule configured with this condition to experience the behavior. |
| Assumptions | |

| Condition | System - Check Integer Property |
| --- | --- |
| Available since version | 10.1.4.5 |
| Checkpoints | All Checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Value | Can be Null? |
| --- | --- | --- | --- |
| Property | The complete name of the property that must be checked. | | Yes |
| PropertyValue | The expected value of the property. If the property has this value then the condition will evaluate to true. | Integer | Yes |
| Defaultvalue | The value of the property to be used if the property is not found in the system. | Integer | Yes |

**Possible Scenarios**

Use this condition when you want to determine whether the value of a particular property equals the expected integer value.

For example, you might have a property "trigger.sample.rule.test.integer" and its value to 25.

You want to trigger some rule based on this property.

For accomplish this, you must use this rule with this condition.

1.  Configure the "Property" of this condition to "trigger.sample.rule.test.integer". Configure the PropertyValue to "25".

2.  Configure DefaultValue to "30"

3.  Run authentication users to see the rule triggers.

4.  Use the Property editor to change the value of the property "trigger.sample.rule.test.integer" to 88.

5.  Run authentication users again.

    Notice that the rule does not trigger.

### C.2.5.5  System - Check Request Date

General information about the condition is provided in the following table.

| Condition | System - Check Request Date |
| --- | --- |
| Description | Verify if the request date of the transaction or authentication is after a specific date. Notice that only the year, month and day part of the date is used. So basically the "time" portion of the date is ignored when comparing dates. |
| Prerequisites | None for condition as such. But you must have rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Value | Can be Null? |
|-----------|-------------|----------------|--------------|
| Date (MM/dd/yyyy) | The date string which the user wants to check the request date against. | | No |
| Is After Request Date | To check to see whether the specified date is after the request date or not after request date | [True] / False | Yes |
| | **Example**: | | |
| | If we suppose that request data is today: | | |
| | Case A | | |
| | Set parameter to false | | |
| | if date entered is < today         it is triggered | | |
| | if date entered is > today         it is not triggered | | |
| | Case B) | | |
| | Set parameter to true | | |
| | if date entered is < today         it is not triggered | | |
| | if date entered is > today         it is triggered | | |

**Example Usage**

Use this condition when you want to determine whether the transaction or authentication occurred after a certain date.

For example, if you want to direct users to a certain other policy after a given date, you might use this rule.

To do this, you must use this rule with this condition.

1.  Configure the "Date" of this condition to "12/22/2009" if you want to trigger a rule starting the 23rd December of 2009.

2.  Configure the "Is After" to "true".

3.  Run authentication on users.

    If the date is after 12/22/2009, the rule triggers.

4.  Using the Policy editor, change the date in this condition to a future date.

5.  Run authentication on the users again.

    Notice that the rule does not trigger.

### C.2.5.6  System - Check String Property

General information about the condition is provided in the following table.

| Condition | System - Check String Property |
|-----------|-------------------------------|
| Description | Verify if specified property equals expected string value |
| Prerequisites | None for condition as such. But you must have rule configured with this condition to experience the behavior. |
| Assumptions | |

| Condition | System - Check String Property |
|---|---|
| Available since version | 10.1.4.5 |
| Checkpoints | All Checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Value | Can be Null? |
|---|---|---|---|
| Property | The complete name of the property that must be checked. | | Yes |
| PropertyValue | The expected value of the property. If the property has this value then the condition will evaluate to true. | String | Yes |
| Defaultvalue | The value of the property to be used if the property is not found in the system. | String | Yes |

**Example Usage**

Use this condition when you want to determine whether the value of a particular property equals the expected the string value.

For example, you have a property "trigger.sample.rule.test.string" and its value is "test_string". You want to trigger a rule based on this property.

For achieving this, you must use this rule with this condition.

1. Configure the "Property" of this condition to "trigger.sample.rule.test.string".

2. Configure the PropertyValue to "test_string" and configure DefaultValue to "some_other_string"

3. Run authentication on users to trigger the rule.

4. Use the Property editor to change the value of the property "trigger.sample.rule.test.instringteger" to "completely different string value".

5. Run authentication on users again.

   Notice that the rule does not trigger.

## C.2.6 Transactions Conditions

These section provides information on the following transaction conditions:

- Transaction: Check Count of Any Entity or Element of a Transaction Using Filter Conditions

- Transaction: Check Current Transaction Using Filter Condition

- Transaction: Check if Consecutive Transactions in Given Duration Satisfy the Filter Conditions

- Transaction: Check Number of Times Entity Used in Transaction.

- Transaction: Check Transaction Aggregrate and Count Using Filter Conditions

- Transaction: Check Transaction Count Using Filter Condition

- Transaction: Compare Transaction Aggregrates (Sum/Avg/Min/Max) Across Two Different Durations

- Transaction: Compare Transaction Counts Across Two Different Durations

- Transaction: Compare Transaction Entity/Element Counts Across Two Different Durations

- Transaction: Check Unique Transaction Entity Count with the specified count

> **Note:** The filter operators "like" and "not like" work only on transaction data and entity data where the data type is string.

### C.2.6.1 Transaction: Check Count of Any Entity or Element of a Transaction Using Filter Conditions

General information about the condition is provided in the following table.

| 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 whether 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. |
| Prerequisites | Ensure that you are using 10.1.4.5.2 or later.<br><br>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 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| 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 must 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 | | |

| 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<br>filter2Key<br>filter3Key<br>filter4Key<br>filter5Key<br>filter6Key | These parameters specify the left hand side of the filter conditions. It represents fully qualified key of the transaction field.<br><br>This field could be an entity field or data field or transaction attribute or request attribute.<br><br>Note: There is a widget for this that renders list box with all the data fields. | | Yes |
| filter1Condition<br>filter2Condition<br>filter3Condition<br>filter4Condition<br>filter5Condition<br>filter6Condition | These parameters represent the operator and right hand side of the filter condition. It represents fully qualified key of the filter condition.<br><br>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 |

**Example Usage**

Use this condition when you want to trigger a rule based on the count of an entity or entity/data element of the transaction.

For example, you configured a transaction called "purchase" and 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 the 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.

### C.2.6.2  Transaction: Check Current Transaction Using Filter Condition

General information about the condition is provided in the following table.

| Condition | Transaction: Check Current Transaction Using Filter |
|---|---|
| Description | Check to see whether the current transaction matches ALL the conditions specified. Up to 6 conditions can be specified. |

| Condition | Transaction: Check Current Transaction Using Filter |
|---|---|
| Prerequisites | 1. Transactions should be defined. <br> 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 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| 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 <br> filter2Key <br> filter3Key <br> filter4Key <br> filter5Key <br> 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. <br><br> This field could be an entity field or data field or transaction attribute or request attribute. | | Yes |
| filter1Condition <br> filter2Condition <br> filter3Condition <br> filter4Condition <br> filter5Condition <br> 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. <br><br> The right hand side is the value, which could be a simple value, the value of the current transaction, or a group. <br><br> ■ Value: A simple value that is entered into a field <br><br> ■ Current: A value from the current transaction. A value is selected from a list of values based on the current entities. <br><br> ■ 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 |

**Example Usage**

This condition can be used whenever you want to trigger a 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).

Dollar amounts must be integer values.

For achieving this, you must 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.

### C.2.6.3  Transaction: Check if Consecutive Transactions in Given Duration Satisfy the Filter Conditions

General information about the condition is provided in the following table.

| Condition | Transaction: Check if Consecutive Transactions in Given Duration Satisfy the Filter Conditions |
|---|---|
| Description | Check to see whether consecutive transactions in a given duration satisfy the specified filter conditions |
| Prerequisites | ■ Transactions should be defined<br>■ Transaction type of the current transaction should be same as the transaction type specified in the rule condition<br>■ Ensure that you are using 10.1.4.5.2 or later. |
| Assumptions | |
| Available since version | 10.1.4.5.2 |
| Checkpoints | All checkpoints. |

#### Parameters

The following table summarizes the parameters in the condition.

| 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.<br><br>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.<br><br>If this value is TRUE then gaps would be allowed while checking for conditions. | | No |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| noOfTransactionsToCheckFor1stCheck | Number of transactions that should satisfy the 1st check. Specify positive integers. | | No |
| filter101Key | Filter Keys for 1st check. | | Yes |
| filter102Key | These parameters specify the left hand side of the filter conditions. It represents fully qualified key of the transaction field. | | |
| filter103Key | | | |
| filter104Key | | | |
| filter105Key | This field could be an entity field or data field or transaction attribute or request attribute. | | |
| filter106Key | | | |
| | Note: There is a widget for this that renders list box with all the data fields. | | |
| filter101Condition | Filter Conditions for 1st check. | | Wherever the filterKey is specified, appropriate condition has to be specified |
| filter102Condition | These parameters represent the operator and right hand side of the filter condition. It represents fully qualified key of the filter condition. | | |
| filter103Condition | | | |
| filter104Condition | | | |
| filter105Condition | 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. | | |
| filter106Condition | | | |
| noOfTransactionsToCheckFor2ndCheck | Number of transactions that should satisfy the 2nd check. Specify positive integers. | | No |
| filter201Key | Filter Keys for 2nd check. | | |
| filter202Key | These parameters specify the left hand side of the filter conditions. It represents fully qualified key of the transaction field. | | |
| filter203Key | | | |
| filter204Key | | | |
| filter205Key | This field could be an entity field or data field or transaction attribute or request attribute. | | |
| filter206Key | | | |
| | Note: There is a widget for this that renders list box with all the data fields. | | |
| filter201Condition | Filter Conditions for 2nd check. | | Wherever the filterKey is specified, appropriate condition has to be specified |
| filter202Condition | These parameters represent the operator and right hand side of the filter condition. It represents fully qualified key of the filter condition. | | |
| filter203Condition | | | |
| filter204Condition | | | |
| filter205Condition | 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. | | |
| filter206Condition | | | |

**Example Usage**

Use this condition when you want to trigger a rule based on checks that are satisfied on consecutive transactions in a given duration.

For example, you configured a transaction called purchase and want to trigger a rule if the current/last transaction amount is greater than $1000 and there were at least 3 transactions before that where the amount was less than $10.

So, the 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 the first check as "1" and select the condition to check as "Amount" "Greater Than" 1000, since you want to check only one transaction for the large amount.

2. Select the number of transactions for the second 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 the first check and the second check, select "Allow Gaps in Transactions during checks?" as TRUE otherwise select FALSE.

### C.2.6.4 Transaction: Check Number of Times Entity Used in Transaction.

General information about the condition is provided in the following table.

| Condition | Transaction: Check Number of Times Entity Used in Transaction. |
| --- | --- |
| Description | Compares the number of times an entity used has been used with the specified count. |
| Prerequisites | |
| | ■ 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 | 11.1.2.0 |
| Checkpoints | All Checkpoints. |

#### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
| --- | --- | --- | --- |
| trxDefFQKey | Transaction Definition fully qualified key. This is specified using list box that has list of transaction definitions | | No |
| entityDefFQKey | Select the entity/element to be counted. Only distinct values will be counted | | No |
| specifiedConditionEnum | Specified Condition | | No |
| specifiedCount | Count value to check. Specify only valid positive integers. | | No |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| durationDescriptor | Specify the duration during which the transactions have to be counted. Duration descriptor widget renders the UI for specify the duration.<br><br>**Important:** By default durationType is 'rolling' meaning it takes current time as the end point to count the start point.<br><br>Therefore, if you specify 1 hour using 'rolling' durationType, it simply subtracts 60 minutes from the current time to compute the start time of the duration window.<br><br>Whenever the duration is described as 'last' x seconds/minutes/hours/days rolling Type duration has to be used.<br><br>There will be occasions where you want to start the duration window start at zero, and then you should use the durationType as 'calendar'.<br><br>For example, suppose the current time is 3.35pm and you want to count behavior that happened between 3pm and 3.35 pm then you can specify it has 1 hour with durationType as 'calendar'. | | No |
| transactionStatusEnum | Specify the transaction status that has to be considered for counting. If you want to consider all transactions regardless of their status then don't specify any status | | Yes |
| ignoreCurrentTransactionInCount | Flag to indicate if the current transaction has to be ignored | | Yes |

**Example Usage**

This condition can be used whenever you want to trigger a rule based on the number of times the same entity has been used over a specified time period.

For example, you have configured a transaction called purchase and you want to trigger if a credit card is used more than 10 times in one day.

To achieve this, select 'Credit card' as the element to be counted and select 1st duration as 1 calendar day.

Then select comparison condition as 'Greater than' and the specified count as 10.

### C.2.6.5 Transaction: Check Transaction Aggregrate and Count Using Filter Conditions

General information about the condition is provided in the following table.

| Condition | Transaction: Check Transaction Aggregrate and Count Using Filter |
|---|---|
| Description | Check the aggregate 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 and so on. |
| Prerequisites | Transactions should be defined.<br><br>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 |

| Condition | Transaction: Check Transaction Aggregrate and Count Using Filter |
|---|---|
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| 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 enables you to specify the duration. | | No |
| | **Important:** By default, durationType is "rolling," meaning it takes the current time as the end point to count backward 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 backward 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. | | |

| 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<br>filter2Key<br>filter3Key<br>filter4Key<br>filter5Key<br>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.<br><br>This field could be an entity field or data field or transaction attribute or request attribute. | | |
| filter1Condition<br>filter2Condition<br>filter3Condition<br>filter4Condition<br>filter5Condition<br>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.<br><br>The right hand side is the value, which could be a simple value, the value of the current transaction, or a group.<br><br>■ Value: A simple value that is entered into a field<br><br>■ Current: A value from the current transaction. A value is selected from a list of values based on the current entities.<br><br>■ 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 |

### Example Usage

Use this condition when you want to trigger a rule based on an aggregate of a transaction numeric value and transaction count.

This is designed to reduce the 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 a lot of purchases (for example, more than 2 per hour with average amount that is greater than 500) from a high-risk country.

For achieving this, you must 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 the 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

### C.2.6.6  Transaction: Check Transaction Count Using Filter Condition

General information about the condition is provided in the following table.

| 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 and so on. |
| Prerequisites | ■ Transactions should be defined. <br> ■ 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 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| 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 |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| 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 enables you to specify the duration. | | No |
| | **Important:** By default, durationType is "rolling," meaning it takes the current time as the end point to count backward 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 backward 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. | | |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| transactionStatusEnum | Specify the transaction status that has to be considered for counting.<br><br>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.<br><br>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.<br><br>If the filter conditions fail on the current transaction, then the rule condition is evaluated to false without performing the count. | | |
| filter1Key<br>filter2Key<br>filter3Key<br>filter4Key<br>filter5Key<br>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.<br><br>This field could be an entity field or data field or transaction attribute or request attribute. | | Yes |
| filter1Condition<br>filter2Condition<br>filter3Condition<br>filter4Condition<br>filter5Condition<br>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.<br><br>The right hand side is the value, which could be a simple value, the value of the current transaction, or a group.<br><br>■ Value: A simple value that is entered into a field<br><br>■ Current: A value from the current transaction. A value is selected from a list of values based on the current entities.<br><br>■ 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 |

**Example Usage**

Use this condition when you want to trigger a rule based on transaction count condition.

For example, suppose you have configured a transaction called "purchase" and you want to challenge the user if the user is performing a lot of purchases (for example

more than 2 per hour with amount greater than 1000 for each purchase) from a high risk country, you may want to use this condition.

For achieving this, you must 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. Configure two filter conditions:

   - One for checking if the amount field is greater than 1000.

   - Another 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.

### C.2.6.7 Transaction: Compare Transaction Aggregrates (Sum/Avg/Min/Max) Across Two Different Durations

General information about the condition is provided in the following table.

| Condition | Transaction: Compare Transaction Aggregrates (Sum/Avg/Min/Max) Across Two Different Durations |
|---|---|
| Description | Compare transactions aggregrates across two different durations |
| Prerequisites | <ul><li>Transactions should be defined</li><li>Transaction entity/data field that has to be aggregrated should be of type numeric</li><li>Transaction type of the current transaction should be same as the transaction type specified in the rule condition</li><li>Ensure that you are using 10.1.4.5.2 or later.</li></ul> |
| Assumptions | |
| Available since version | 10.1.4.5.2 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| 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 must be aggregrated | | No |
| durationDescriptorFor1stDuration | Select duration for the first aggregrate | | No |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| 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 |
| 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 filter4Key filter5Key filter6Key | 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. | | Yes |
| 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 |

**Example Usage**

Use this condition when 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 configured a transaction called purchase and want to trigger if the sum of the transaction amount for the current day is 20% more than the sum of all transactions amount of the 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 first duration as 1 calendar day and the second duration as 1 calendar day before 1 day.

3. Then select the comparison condition as "Greater than" and multiplier value as 1.2 (100%+20%).

### C.2.6.8 Transaction: Compare Transaction Counts Across Two Different Durations

General information about the condition is provided in the following table.

| Condition | Transaction: Compare Transaction Counts Across Two Different Durations |
|---|---|
| Description | Compare transactions counts across two different durations |
| Prerequisites | ■ 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 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| 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 |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| filter1Key<br>filter2Key<br>filter3Key<br><br>filter4Key<br>filter5Key<br>filter6Key | These parameters specify the left hand side of the filter conditions. It represents fully qualified key of the transaction field.<br><br>This field could be an entity field or data field or transaction attribute or request attribute.<br><br>Note: There is a widget for this that renders list box with all the data fields. | | Yes |
| filter1Condition<br>filter2Condition<br>filter3Condition<br><br>filter4Condition<br>filter5Condition<br>filter6Condition | These parameters represent the operator and right hand side of the filter condition. It represents fully qualified key of the filter condition.<br><br>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 |

**Example Usage**

Use this condition when you want to trigger a rule based on the comparison of transaction counts across two different durations.

For example, you configured a transaction called "purchase" and want to trigger the rule 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 the first duration as 1 calendar day and the second 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%).

### C.2.6.9  Transaction: Compare Transaction Entity/Element Counts Across Two Different Durations

General information about the condition is provided in the following table.

| Condition | Transaction: Compare Transaction Entity/Element Counts Across Two Different Durations |
|---|---|
| Description | Compare transaction entity/element counts across two different durations |
| Prerequisites | ■  Transactions should be defined<br>■  Transaction type of the current transaction should be same as the transaction type specified in the rule condition<br>■  Ensure that you are using 10.1.4.5.2 or later. |
| Assumptions | |
| Available since version | 10.1.4.5.2 |
| Checkpoints | All checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| 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 filter4Key filter5Key filter6Key | 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. | | Yes |
| 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 |

**Example Usage**

Use this condition when you want to trigger a rule based on the comparison of any transaction entity/element counts across two different durations.

For example, you configured a transaction called "purchase" and 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 accomplish this:

1. Select "Credit card" as the element to be counted and select the first duration as 1 calendar day and the second 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%).

### C.2.6.10  Transaction: Check Unique Transaction Entity Count with the specified count

General information about the condition is provided in the following table.

| Condition | Transaction: Check Unique Transaction Entity Count with the specified count |
|---|---|
| Description | Check Unique Transaction Entity Count with the specified count |
| Prerequisites | |
| | ■ 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 |
| Checkpoints | All Checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| trxDefFQKey (Select Transaction) | Transaction Definition fully qualified key. This is specified using list box that has list of transaction definitions | Select one from list presented on the screen | No |
| entityDefFQKey (Select Transaction Entity to count) | Select the entity/element to be counted. Only distinct values will be counted | | No |
| specifiedConditionEnum | Specified Condition | Select from drop down list. | No |

| Parameter | Description | Possible Values | Can be Null? |
|-----------|-------------|-----------------|--------------|
| durationDescriptor | Specify the duration during which the transactions must be counted. The duration descriptor field shows types of durations you can choose from in the user interface.<br><br>Important: By default the durationType is `rolling`, meaning it takes the current time as the end point to count the start point.<br><br>If you specify 1 hour using the `rolling` durationType, it subtracts 60 minutes from the current time to compute the start time of the duration window.<br><br>Whenever the duration is described as **last** x seconds/minutes/hours/days, the rolling type duration has to be used.<br><br>There will be occasions where you want to start the duration window **start at zero**, then you should use the durationType as **calendar**.<br><br>For example, if the current time is 3.35pm and you want to count something that happened between 3pm and 3.35 pm, then you can specify it has 1 hour with durationType as **calendar**. | Select from list. | No |
| transactionStatusEnum | This parameter specifies the transaction status to consider for counting. To consider all transactions regardless of their status, do not specify any status | Enumeration from list<br><br>Enumeration element of tracker.transaction.status.enum | Yes |
| forCurrentUser | This parameter specifies whether to evaluate the condition for the current users | Boolean. True or False | No |
| ignoreCurrentTransactionInCount | Flag to indicate if the current transaction has to be ignored | | Yes |

**Example Usage**

This condition can be used whenever you want to trigger a rule based on the number of times the same entity has been used over a specified time period.

For example, you have configured a transaction called "Purchase" and you want to trigger if a credit card is used more than 10 times in one day by the same user. To achieve this, proceed as follows:

1. Select **Credit card** as the element to be counted and select 1st duration as 1 calendar day.

2. Select forSame User as **True**.

3. Then select the comparison condition as **Greater than** and the specified count as **10**.

4. Set transactionStatus to **Success**.

5. Select **IgnoreCurrentTransactionCount** to **True**, so that your current transaction will not be counted.

## C.2.7  User Conditions

The following user conditions are documented in this section:

- User: Check If Devices Of Certain Type Are Used
- User: Check User Data
- User: Stale Session
- User: Devices Used
- User: Velocity from Last Success
- User: Check Number of Registered Devices Of Given Type

### C.2.7.1  User: Check If Devices Of Certain Type Are Used

General information about the condition is provided in the following table.

| Condition | User: Check If Devices of a Certain Type are Used |
|---|---|
| Description | Number of devices of given type used in given time. |
| Prerequisites | None for condition as such. But you must have rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 11.1.2.0.0 |
| Checkpoints | All Checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Value | Can be Null? |
|---|---|---|---|
| Number Of Devices | Compare operator for number of actual devices found of given type and the number configured in this condition. | [enumeration] Default is More Than. Possible values are More Than Equal To, Less Than, Less That Equal To, Equal To, Not Equal To | No |
| Number of devices to compare | Provide the number of devices to be compared with the devices to be found for the user. | [Integer] Default is 0. Provide a positive integer number. (Greater than or equal to 0) | No |
| Device Of Type | Select Device type to look for. | [Enumeration] Default is Mobile Device Other possible value is Desktop Device | No |

| Parameter | Description | Possible Value | Can be Null? |
|---|---|---|---|
| Within Duration (seconds) | Time period in seconds to look back into users session history. | [Integer] Default is 3600.<br><br>Positive integer indicates that condition looks for finite time before this request. 0 value will mean that condition will look for all available history of sessions. If negative value is provided for this parameter then condition will always evaluate to false. | No |

### Example Usage

This condition can be used whenever you want to check if the user is using too many devices of certain type in certain time period immediately preceding this request. For example, lets say you want to restrict users to use only N number of mobile devices in last 24 hours.

To achieve this, you need to use this condition in a rule.

1. Configure the "Number of Devices" operator of this condition as "Greater Than." Configure the "Number of Devices to compare value of this condition as "N-1".

2. Configure the "Devices of type" of this condition as "Mobile Device" and configure the "within seconds" of this condition as 86400.

3. Run authentications with the registered users and you can see the rule triggering when they have used "N" devices within last 24 hours.

### C.2.7.2  User: Check User Data

General information about the condition is provided in the following table.

| Condition | User: Check User Data |
|---|---|
| Description | Verify if specified key has any related data for the user |
| Prerequisites | None for condition as such, but you must have rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Checkpoints. |

### Parameters

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Value | Can be Null? |
|---|---|---|---|
| User Data Key | The complete name of the key which may have associated data for that user.<br><br>Consider this a property or a configuration property for only that user. | [Strings] Default is email | Yes |

**Example Usage**

This condition can be used whenever you want to check to see whether the user has associated data for the key. For example, you may want to determine whether the user has an email defined in his OTP configuration, so you want to trigger a rule based on whether this email field is defined (non-empty) for the user. To do this, you must use this rule with this condition.

1. Configure the "User Data Key" of this condition with "user_otpContactInfo_email" (for mobile phone, use key to "user_otpContactInfo_mobile").

2. Use the new out-of-the-box base policies that are shipped with 11*g*. This will force user to register for OTP on the first or second login.

3. Run authentications with the registered users.

   You can see the rule triggering when they are registered for the OTP email (or mobile if you have used that as key).

4. Then go to policy editor and change the value of the key "zoom.some.item.that.is.not.supposed.to.exist."

5. Run authentication users again and notice that the rule does not trigger.

   Notice that the rule does not trigger. (The assumption is that no such key data exists for this usual key)

### C.2.7.3 User: Stale Session

General information about the condition is provided in the following table.

| Condition | User: Stale Session |
|---|---|
| Description | Verify if a newer session is established after this session is created |
| Prerequisites | None for condition as such. But you must have a rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoint | All checkpoints. |

**Example Usage**

This condition can be used whenever you want to determine whether the user has established a successful login from another channel while this authentication is in progress.

### C.2.7.4 User: Devices Used

| Condition | User: Devices Used |
|---|---|
| Description | Number of devices tried in given time |
| Prerequisites | None for condition as such, but you must have rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Value | Can be Null? |
|---|---|---|---|
| Number of devices | Provide the number of devices to be compared with the devices to be found for the user. | [Integer] Default = 0.<br><br>Provide a positive integer number. (>=0) | No |
| Within Duration (seconds) | Time period in seconds to look back into users session history. | [Integer] Default = 3600.<br><br>Positive integer indicates that condition looks for finite time before this request. 0 value will mean that condition will look for all available history of sessions. If negative value is provided for this parameter then condition will always evaluate to false. | No |

**Example Usage**

This condition can be used whenever you want to check if the user is using too many devices in certain time period immediately preceding this request.

For example, you want to restrict users to use only N number of devices in last 24 hours.

To achieve this, you need to use this condition in a rule.

1. Configure the "Number of Devices to compare" value of this condition = "N-1".

2. Configure the "within seconds" of this condition = 86400.

3. Run authentications with the registered users and you can see the rule triggering when they have used "N" devices within last 24 hours.

### C.2.7.5 User: Velocity from Last Success

General information about the condition is provided in the following table.

*Table C–8   User: Velocity from Last Success*

| Condition | User: Velocity from Last Success |
|---|---|
| Description | Condition evaluates to check to see if<br><br>■　The user's login was successful earlier, and<br><br>■　The velocity in miles per hour is more than the specified value, and<br><br>■　The user belongs to the same Device ID |
| Prerequisites | None for condition as such, but you must have the rule configured with this condition |
| Assumptions | |
| Available since version | 10.1.4.5 |
| Checkpoints | All Checkpoints. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Value | Can be Null? |
|---|---|---|---|
| Miles per hour is more than | The velocity in miles per hour is more than specified value | Positive integer<br><br>Default: 60 | No |
| ignore if last login device is same | See possible value. | True/False<br><br>The flag is set to true<br><br>■ if there are more than one successful login from the same user from the same Device ID. The condition returns false and no action/alert is triggered.<br><br>■ if there are more than one successful login from the same user from different Device IDs and the condition returns true and an action/alert is generated.<br><br>The flag is set to false<br><br>`False` ignores the parameter and the condition evaluates based on miles per hour only. | Yes |
| Exclude IP List | This parameter allows you to specify a list of IPs to ignore. If a user's IP is from that list, then this condition always evaluates to false. If the user's IP is not in that list or if the list is null or empty, then the condition evaluates the velocity of the user or the device from the last login and evaluates to true if the velocity exceeds the configured value. | | |

### Scenario

Condition evaluates if the users login was successful earlier and the velocity in miles per hour is more than specified value and user belong to the same Device ID. If there are multiple logins of the same user from the same device, then the parameter "ignore if last login device is same" will act. In order for the condition to be false, there must be multiple logins that are successful from the same user that is using the same Device ID. The location database is used to determine the location of the user for this login and the previous login.

### Use Case 1

User: karen1, Device ID: 2106, Previous Device ID: None, rule-flag: true

1. Log in from device from IP1

2. Log in from the same device from IP2 (which is 60 miles away). There is no alert generated.

3. Log in from the same device and IP2 (which is 60 miles away). There is no alert generated.

**Table C–9    Use Case 1**

| User name | Auth Status | Device ID | Location | IP | Alert |
|---|---|---|---|---|---|
| karen1 | Success | 2106 | US, Texas, Austin | IP1 | No alert |
| karen1 | Success | 2106 | US, Arizona, Gila Bend | IP2 | No alert. An alert is not generated since the same user has the same device and the flag is set to true. |
| karen1 | Success | 2106 | US, Arizona, Gila Bend | IP2 | No alert. An alert is not generated since the same user has the same device and the flag is set to true. |

**Use Case 2**

User: karen1, Device ID: 2107, Previous Device ID: 2106, rule-flag: true

1. Log in from the same device from IP1.

2. Log in from the same device from IP2 (which is 60 miles away). There is no alert triggered.

3. Log in from the same device and IP2 (which is 60 miles away). There is no alert triggered.

**Table C–10    Use Case 2**

| User name | Auth Status | Device ID | Location | IP | Alert |
|---|---|---|---|---|---|
| karen1 | Success | 2107 | US, Arizona, Gila Bend | IP1 | New device |
| karen1 | Success | 2107 | US, Texas, Austin | IP2 | No alert. An alert is not generated since the same user has the same device and the flag is set to true. |
| karen1 | Success | 2107 | US, Texas, Austin | IP2 | No alert. An alert is not generated since the same user has the same device and the flag is set to true. |

**Use Case 3**

User: karen1, Device ID: 2109, Previous Device ID: 2108, rule-flag: false

1. Log in from Device 2108 from IP1.

2. Log in from Device 2109 from IP2 (which is 60 miles away). Alerts are triggered.

3. Log in from the same device (Device 2109) and IP2 (which is 60 miles away). No alert is triggered.

**Table C–11    Use Case 3**

| User name | Auth Status | Device ID | Location | IP | Alert |
|---|---|---|---|---|---|
| karen1 | Success | 2108 | US, Texas, Austin | IP1 | New device |
| karen1 | Success | 2109 | US, Arizona, Gila Bend | IP2 | Device High Velocity<br>User High Velocity |
| karen1 | Success | 2109 | US, Arizona, Gila Bend | IP2 | No alert |

### C.2.7.6 Understanding How the OAAM Device Max Velocity Rule Settings Work

The "Device Max Velocity" rule is used to detect "man in the middle" attacks where a hacker obtains the MAC address for devices that users log in from. Hackers replay the user's login and provide the user's computer MAC address. By doing this they fool the system into thinking the user is logging in from a known and trusted device that is in the user's OAAM profile.

The "Device Max Velocity" rule can detect this type of attack, trigger an alert and block the hacker from successfully signing in. This is accomplished in conjunction with the Quova subscription data. The rule checks to see if the MAC address is in the list of known devices the user is logged in from. Then it examines the IP address location where the user is logged in from. If a hacker then tries to log in by replaying the user's session and also using the user's device MAC address from another location, such as 100 miles away, the rule uses a formula that determines the possibility of that user's device traveling at that velocity.

It is possible for a user to log in to his application, then take a Jet to fly to another city and once again log in to the same application. Therefore you want to be able to adjust the variables of the formula to allow for a portable device to travel at least the speed of a Jet. The "Device Max Velocity" rule has two values that the administrator can configure. Those value fields are called "Last Login Within (Seconds)" and "Miles Per Hour is More Than". Using these two field values you can customize the allotted velocity that a physical device can travel before an alert is triggered.

#### How the Rule Formula Works

1. The rule first picks up the last successful login in the last N seconds. (If there are multiples, the last one (with the highest timestamp) is picked.

2. The rule looks at cityLastLogin and currentCurrentLogin and calculate the distance between them which "= the distance."

3. Then it calculates thisDistance divided by the difference in login times. That becomes the velocityCalculated.

4. If velocityCalculated is more than velocityConfigured in the rule (from the user interface), the rule triggers.

#### Solution

Using the following testing assumptions and steps you can make the "Device Max Velocity" rule alert trigger, and also see how to avoid not triggering the rule alert. Before starting your test:

The user's auth status should be "success" in the previous login (N seconds ago).

Assume you only have one minute to test the "Device Max Velocity" rule. Assuming that point A and point B are 900 miles apart, in order to travel from point A to point B in 60 seconds, you need to be traveling at 54000 miles an hour.

1. Set your "Miles Per Hour is More Than" to 54000

2. Set the "Last Login Within (Seconds)" to 60 seconds.

*Setting up the Test*:

Pick two IP addresses for the test that you know are far away from each other. You are using the following IP addresses from the Quova data:

63.232.120.161 Austin, Texas

63.229.250.34 Phoenix, Arizona

These two cities are a distance of 867 miles apart.

Make sure that the rule is not triggered by logging in twice and not exceeding the "Device Max Velocity" settings you already set to 60 seconds and 54000 miles per hour. Log in twice with the same user and device with logins no less than 75 seconds apart. Make sure that each time you log in you use a tool like Firefox "Modify Headers" to change the IP address between logins using the two IP Addresses mentioned earlier in this section. This simulates a device logging in from two different locations 867 miles apart. The Device Max Velocity alert does not trigger.

Now perform the same test again where you log in twice less than 30 seconds apart, again, changing the IP address between logins. The Device Velocity alert is triggered.

Understanding the relationship between the "Miles Per Hour is More Than" and the "Last Login Within (Seconds)" settings: You cannot change one of these settings and not consider what the other needs to be set to. In other words, you cannot only set the "Mile Per Hour is More Than" setting and not properly adjust the "Last Login within (Seconds)" setting. These two settings work together with the formula to calculate a devices velocity. The relationship between these two settings is not an "OR". It is an "AND". Last Login AND Mile per hour work together. Remember the following two rules before changing these two settings.

1.  You cannot only consider the "Miles Per hour" when setting the velocity. You must also consider the "Last Login within (Seconds)" setting.

2.  When testing, you must consider and calculate the distance between point A and point B, the time taken to conduct the test, and further factor in the distance between the two points and how long the testing takes. If you want to use one minute as the time allotted for the testing, then make sure you know the distance between point A and Point B. You must also know how long it takes to get from point A and point B in 60 seconds, again, if you plan to conduct your test in less than one minute.

### C.2.7.7 User: Check Number of Registered Devices Of Given Type

General information about the condition is provided in the following table.

| Condition | User: Check Number of Registered Devices Of Given Type |
| --- | --- |
| Description | Number of registered devices of given type. |
| Prerequisites | None for condition as such, but you must have the rule configured with this condition to experience the behavior. |
| Assumptions | |
| Available since version | 11.1.2.0.0 |
| Checkpoints | All Runtimes. |

**Parameters**

The following table summarizes the parameters in the condition.

| Parameter | Description | Possible Values | Can be Null? |
| --- | --- | --- | --- |
| Compare Number Of Devices | Compare operator for number of actual registered devices found of given type and the number configured in this condition | [enumeration] Default= More Than<br><br>More Than Equal To, Less Than, Less That Equal To,<br><br>Equal To, Not Equal To | No |

| Parameter | Description | Possible Values | Can be Null? |
|---|---|---|---|
| Number of (registered) devices to compare | Number of devices to compare. | [Integer] Default = 4<br><br>Provide a positive number. I this number is less than zero the condition will always evaluate to false. | No |
| Device of Type | Select Device type to look for. | [Enumeration] Default = Mobile Device<br><br>Other possible value is Desktop Device | No |

**Example Usage**

This condition can be used whenever you want to check if the user has too many devices registered.

For example, you want to restrict users to use only N number of registered mobile devices.

To achieve this, you need to use this condition in a rule.

Configure the "Number of Devices" operator of this condition as "Greater Than. Configure the "Number of Devices to compare" value of this condition as "4".

Configure the "Devices of type" of this condition as "Mobile Device".

Run a few authentications with the registered users from a new device every time (clear cookies) register those devices for the user.

When user has 5 devices registered and comes in from either a new or an existing device, the rule will be triggered.

# D

# Oracle Adaptive Access Manager Reports Reference

Reports are available for the following topics in Oracle Adaptive Access Manager:

- Common Reports
- Devices Reports
- KBA Reports
- Location Reports
- Performance Reports
- Security Reports
- Summary Reports
- Users Reports

## D.1 Common Reports

These reports provide data based on device location or login information.

| Report Name | Description |
|---|---|
| RecentLogins | Lists all logins in the specified time range. |

## D.2 Devices Reports

These reports provide data based on the device information.

| Report Name | Description |
|---|---|
| DeviceIdScoring | Displays Device ID scoring summary for the designated date range. |
| MultipleFailures | Lists all devices with multiple login failures in the specified time range. |
| MultipleUsers | Lists all devices that have multiple users. |

## D.3 KBA Reports

These reports provide data based on the KBA information.

| Report Name | Description |
|---|---|
| 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. |

> **Note:** Updated statistics are not available immediately after a user is challenged or answers a question. The BI Publisher reports are generated from the database and database updates do not occur in real-time for the statistics.

## D.4 Location Reports

These reports provide data based on the location information.

| Report Name | Description |
|---|---|
| CountryAggregates | Displays country aggregate summary for the designated date range. |
| MultipleUsers | Lists all locations that have multiple users. |
| StateAggregates | Displays state aggregate summary for the designated date range. |

## D.5 Performance Reports

These reports provide data based on the performance information.

| Report Name | Description |
|---|---|
| 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. |

## D.6 Security Reports

These reports provide data based on the security information.

| Report Name | Description |
|---|---|
| AlertsBreakdown | Displays alert breakdown summary for the designated date range. |
| PostAuthScoring | Displays post-authorization scoring summary for the designated date range. |
| PreAuthScoring | Displays pre-authorization scoring summary for the designated date range. |

| Report Name | Description |
| --- | --- |
| RulesBreakdown | Displays rules breakdown summary for the designated date range. |
| ScoringCombinations | Displays score combination summary for the designated date range. |

## D.7  Summary Reports

These reports provide summaries for date ranges.

| Report Name | Description |
| --- | --- |
| AveragesSummary | Displays average summary for the designated date range. |
| LoginSummary | Displays login aggregate summary for the designated date range. |

## D.8  Users Reports

These reports provide data based on the user information.

| Report Name | Description |
| --- | --- |
| MultipleDevices | Lists all users that use multiple devices. |

# E

# The Discovery and OAAM Policy Development Processes

This appendix shows the security policy development process and the modeling process in which high-level requirements are translated into security policies.

It contains the following sections:

- Security Policy Development Process
- Discovery Process Overview
- Example Scenario: Transaction Security
- Example Scenario: Login Security

## E.1 Security Policy Development Process

The process for developing policies are outlined in this section.

### E.1.1 Overview

Table E–1 summarizes examples of actors who would take part in the security policy development process.

*Table E–1    Example of Policy Development Actors*

| Actors | Description |
| --- | --- |
| Investigators and Customer Service Representatives | Investigators and Customer Service Representatives (CSR) use Oracle Adaptive Access Manager's case management tools to handle security and customers cases day-to-day. They have detailed knowledge about user activity and security issues. Analysts work with investigators and CSRs to identify if policies need to be adjusted or new policies need to be created. |
| Business/Security Analyst | Analysts gather intelligence from various sources to identify needs and develop requirements to address them. Some sources for intelligence include Investigators, industry reports, antifraud networks, compliance mandates, and company polices. |
| Security Administrator | Administrators plan, configure and deploy policies based on the requirements from analysts. |
| System Administrator | A System Administrator configures environment-level properties and transactions. |
| Quality Assurance | Quality Assurance (QA) tests the policies to confirm that they meet requirements. |

**Edits to existing policy**

Editing an existing policy involves the following tasks:

- Research/Troubleshooting

- Requirements and Planning
- Configuration
- Testing
- Deployment to production

**Creating a New Policy**

Creating a new policy involves the following tasks:

- Discovery/Research
- Requirements and Planning
- Configuration
- Testing
- Deployment to production

## E.1.2 Edit Policy: Research/Troubleshooting

Business Analysts gather intelligence from various sources to identify issues and develop requirements to address them.

*Table E–2    Edit Policy: Research/Troubleshooting*

| Source | Details |
|---|---|
| OAAM Reports | In an existing OAAM deployment analysts can run reports using BIP to identify security or customer issues that need to be addressed. |
| Investigator/CSR feedback | Interviews with staff can reveal customer and security issues. Are customers complaining they are challenged too often without valid cause? Are there a number of fraud cases where the current policy was not strict enough to prevent access? |
| Industry Reports | There may be a new type of threat not covered by the current rules. Do thresholds need to be adjusted? |
| Anti-Fraud Networks | Are there new rule thresholds being suggested by peers/experts? Do they make sense for the business? |

## E.1.3 New Policy: Discovery/Research

Business and Security Analysts gather intelligence from various sources to identify needs and develop requirements to address them.

*Table E–3    New Policy: Discovery/Research*

| Source | Details |
|---|---|
| OAAM Reports | In an existing OAAM deployment analysts can run reports using BIP to identify security or customer issues that need to be addressed. |
| Investigator/CSR feedback | Interviews with staff can reveal customer and security issues. Are customers complaining they are challenged too often without valid cause? Are there a number of fraud cases where current policy was not strict enough to prevent access? |
| Industry Reports | There may be a new type of threat not covered by the current rules. Do thresholds need to be adjusted? |

*Table E–3    (Cont.)  New Policy: Discovery/Research*

| Source | Details |
| --- | --- |
| Anti-Fraud Networks | Are there new rule thresholds being suggested by peers/experts? Do they make sense for your business? |
| Compliance | Is there a new mandate for security measures not addressed by your current policies? |
| Company policy | Are there new requirements for employee access that can be addressed with OAAM? |

## E.1.4  Edit/New Policy: Requirements and Planning

Business/Security Analysts develop requirements to address needs identified during discovery.

- What new policies are needed and why?

- What are the use cases?

- What are the expected outcomes (actions, alerts, score)?

- What applications are involved?

- What user groups are involved?

## E.1.5  Edit/New Policy: Configuration

Security Administrators plan, configure and deploy policies based on the requirements from analysts.

- What data points should be profiled by autolearning?

- What rules need to be configured to fulfill use cases?

- What thresholds should be defined for rules?

- What rule outcomes are needed?

## E.1.6  Edit/New Policy: Testing

QA tests the policies to confirm that they meet requirements.

- Do the expected outcomes occur?

- Are the rule thresholds triggering as expected?

- Is the profiling working as expected?

- Following common "normal" end user flows, do the new polices cause user experience issues? Too many challenges, users blocked, and so on.

- Offline can be used to test new/edited policy based on historical control date.

## E.1.7  Edit/New Policy: Deployment to Production

Security Administrator:

- Deploy new policies to the production environment once QA has signed off.

- Export policy set and groups from dev/QA environment

- Import to production

## E.2 Discovery Process Overview

The high-level steps involved in security policy development are as follows:

1. Determine what you are trying to accomplish (problem statement).

2. Break the problem statement into:

   - Inputs: What data is available to evaluate?

   - Rules: What types of evaluations do I need to perform on the data?

   - Outcomes: What should happen based on the analysis?

3. Translate the wording of the problem statement into a security policy by mapping the data, evaluations, and outcomes to an OAAM configuration.

4. Configure entities, transactions, patterns, groups, policies, rules, actions and alerts based on the above preparation.

## E.3 Example Scenario: Transaction Security

In this scenario, a Security Administrator must configure OAAM to notify the security team if there are more than 4 orders to a shipping address in a 24 hour period.

### E.3.1 Problem Statement

Notify the security team to perform a manual review if there are more than 4 orders placed to any single shipping address in a 24 hour period regardless of the number of users.

### E.3.2 Inputs Available

The following data is required to perform the stated evaluation described in the problem statement:

- Date/time of each order

- Shipping address for each order

- Count of orders using each shipping address

### E.3.3 Evaluation

It is recommended to form a logical statement to describe the risk evaluation required by your problem statement.

The logical statement for this scenario is:

"For a shipping address, if total # of orders > 4 in last 24 hours, then review order."

### E.3.4 Outcomes

The outcome required by the problem statement in this case is to generate a single Fraud Alert for the security team.

### E.3.5 Translation

In the translation step, the problem statement that was broken down is mapped to the OAAM security policy components.

*Table E–4    Problem Statement Mapping*

| Problem Statement Breakdown | Oracle Adaptive Access Manager Security Policy Components |
| --- | --- |
| Notify the security team to perform a manual review | An alert with specific messaging |
| Shipping address | An address entity |
| Orders | A custom checkpoint for this transaction is needed |
| | A policy scoped to the "order" checkpoint will contain any rules needed. |
| If there are more than 4 orders placed to any single shipping address in a 24 hour period | A rule configured using a generic transaction rule condition |

### E.3.6  Alert

The best practice is for every evaluation to have a separate alert message.

## E.4  Example Scenario: Login Security

In this scenario, a Security Administrator wants users that login from a state they have used less than 5% of the time in the last month to answer a KBA challenge question before being allowed into the protected application.

### E.4.1  Problem Statement

Profile users' login behaviors including the geographic locations they login from. Use their unique profile to determine how risky a login attempt is and challenge with a KBA question when required based on risk level. If the login is from a state the user have come from less than 5% of the time in the last month them with a KBA challenge before allowing them into the protected application.

### E.4.2  Inputs Available

The following data is required to perform the stated evaluation described in the problem statement:

- User
- Time period
- Geographic location
- Percentage for total logins used for the comparison
- Registration status

### E.4.3  Evaluation

It is recommended to form a logical statement to describe the risk evaluation required by your problem statement.

The logical statement for this scenario is:

"For a user (logging in from state(s)), if % of logins < 5% of all his logins from this state in last month, then challenge user."

### E.4.4 Outcome

The outcome required by the problem statement in this case is to challenge the user with a KBA question if the percentage of logins to a state is less than 5% of his total log ins to states in the last month.

### E.4.5 Translation

In the translation step, the problem statement that was broken down is mapped to the OAAM security policy components.

*Table E–5    Problem Statement Mapping*

| Problem Statement Breakdown | Oracle Adaptive Access Manager Security Policy Components |
|---|---|
| if logins from a state | Pattern to track the user's logins from different states. |
| | Multi-bucket pattern with user as actor and state as attribute and for each as the compare operator. |
| challenge user | An action group to KBA Challenge |
| with a KBA question | Is registered is an attributes and equals as the compare operator and yes as the compare value. |
| | He has to have questions registered before the system can challenge him with a KBA question |
| percentage for state vs. percentage of total | Condition: "Pattern (Authentication): Entity is Member of Pattern Less Than Some Percent Time" |
| 5% | Percentage basis specified in rule |
| last 1 month | Time period specified in rule |
| before allow to proceed to protected resource | Post-Authentication checkpoint policy |
| | In best practices, KBA challenges occur in the Post-Authentication checkpoint. |

### E.4.6 Action

KBA challenge users logging in from a state that they do not log in from, specifically one that they use less than 5% of their total logins to states in a month

# F

# Globalization Support

This chapter provides information on customizing Oracle Adaptive Access Manager for your locale.

## F.1 Supported Languages

Oracle Adaptive Access Manager 11*g* is translated into 9 Admin languages for OAAM Admin and 26 languages for OAAM Server. These translations are bundled along with the English version of the product.

The languages and their locale identifiers (in parentheses) are listed below. A locale identifier consists of at least a language identifier, and a region identifier (if required).

OAAM Admin is translated into French (fr), German (de), Italian (it), Spanish (es), Brazilian Portuguese (pt_br), Japanese (ja), Korean (ko), Simplified Chinese (zh_cn), and Traditional Chinese (zh_tw).

When one of the non-OAAM Admin locale languages is set in the browser (for example Arabic), OAAM Admin uses the default locale, English. When one of the non-standard runtime locale languages is set in the browser, OAAM Server uses the default locale, English.

OAAM Server is translated into 26 languages: French (fr), German (de), Italian (it), Spanish (es), Brazilian Portuguese (pt_br), Japanese (ja), Korean (ko), Simplified Chinese (zh_cn), Traditional Chinese (zh_tw) Arabic (ar), Czech (cs), Danish (da), Dutch (nl), Finnish (fi), Greek (el), Hebrew (iw), Hungarian (hu), Norwegian (no), Polish (pl), Portuguese (pt), Romanian (ro), Russian (ru), Slovak (sk), Swedish (sv), Thai (th), and Turkish (tr).

## F.2 Turning Off Localization

There is no flag to turn-off localization, but there is a property that captures the locales supported by the deployment. The property can be used to enable only one locale.

You would change the `locale.enum.XXX.adminSupported` and `locale.enum.XXX.enabled` properties to `false` for each unwanted locale.

## F.3 Configuring Language Defaults for Oracle Adaptive Access Manager

You can configure language defaults in the `client_resource_<locale>.properties` file using the `bharosa.locale. enum` property. Refer to "Extending/Customizing OAAM" in *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager* for instructions on customizing Oracle Adaptive Access Manager.

An example of a `bharosa.locale.` enum is shown here:

```
bharosa.locale.enum.german=2
bharosa.locale.enum.german.name=German
bharosa.locale.enum.german.description=German
bharosa.locale.enum.german.language=de
bharosa.locale.enum.german.country=
bharosa.locale.enum.german.adminSupported=true
bharosa.locale.enum.german.enabled=true
```

To enable the default locale:

1. Add and set the `bharosa.local.enum.<locale>.enabled` properties of the locales you want to support to true.

2. Add and set the `bharosa.local.enum.<locale>.enabled` properties of the locales you do not want to support to false.

3. Add and set the `bharosa.default.locale property` to match the `bharosa.locale.enum.<locale> property` of your locale.

> **Note:** The only locales supported are the ones listed in the enums.

## F.3.1 Example 1

A German bank wants to set German as the default language and wants to support only German. To do this, follow these steps for `client_resource_de.properties`:

1. If the locale enum does not exist, create it:

   ```
   bharosa.locale.enum.german.enabled=true
   ```

2. If the locale enum already exists, set it to true.

3. If present, set other `bharosa.local.enum.<locale>.enabled` properties to false.

   ```
   bharosa.locale.enum.italian.enabled=false
   bharosa.locale.enum.french.enabled=false
   bharosa.locale.enum.portuguese_br.enabled=false
   bharosa.locale.enum.spanish.enabled=false
   bharosa.locale.enum.korean.enabled=false
   bharosa.locale.enum.chinese_cn.enabled=false
   bharosa.locale.enum.chinese_tw.enabled=false
   bharosa.locale.enum.japanese.enabled=false
   bharosa.locale.enum.arabic.enabled=false
   bharosa.locale.enum.czech.enabled=false
   bharosa.locale.enum.danish.enabled=false
   bharosa.locale.enum.dutch.enabled=false
   bharosa.locale.enum.finnish.enabled=false
   bharosa.locale.enum.greek.enabled=false
   bharosa.locale.enum.hebrew.enabled=false
   bharosa.locale.enum.hungarian.enabled=false
   bharosa.locale.enum.norwegian.enabled=false
   bharosa.locale.enum.polish.enabled=false
   bharosa.locale.enum.portuguese.enabled=false
   bharosa.locale.enum.romanian.enabled=false
   bharosa.locale.enum.russian.enabled=false
   bharosa.locale.enum.slovak.enabled=false
   ```

```
bharosa.locale.enum.swedish.enabled=false
bharosa.locale.enum.thai.enabled=false
bharosa.locale.enum.turkish.enabled=false
```

4. Set `bharosa.default.locale property` to match the value of the locale enum.

   Since `bharosa.locale.enum.german=2,` set `bharosa.default.locale` property to 2.

   If the property does not exist, create it.

## F.3.2 Example 2

A Brazilian bank wants to set Brazilian Portuguese as the default, but wants to display all the other languages that OAAM Server had been translated to. To do this:

1. If the locale enum does not exist, create it:

   ```
   bharosa.locale.enum.pt_br.enabled=true
   ```

2. If the locale enum already exists, set it to true.

3. Set all other `bharosa.local.enum.<locale>.enabled` properties using the Properties Editor to false.

4. Set `bharosa.default.locale` property to the value of the locale enum using the Properties Editor.

   If `bharosa.locale.enum.pt_br=9,` set `bharosa.default.locale property` to 9.

5. Set `bharosa.locale.enum.<locale>.enabled` property in `client_resource_<locale>.properties` for all the languages OAAM Server had been translated to and ensure they are set to true.

   ```
   bharosa.locale.enum.german.enabled=true
   bharosa.locale.enum.italian.enabled=true
   bharosa.locale.enum.french.enabled=true
   bharosa.locale.enum.portuguese_br.enabled=true
   bharosa.locale.enum.spanish.enabled=true
   bharosa.locale.enum.korean.enabled=true
   bharosa.locale.enum.chinese_cn.enabled=true
   bharosa.locale.enum.chinese_tw.enabled=true
   bharosa.locale.enum.japanese.enabled=true
   bharosa.locale.enum.arabic.enabled=true
   bharosa.locale.enum.czech.enabled=true
   bharosa.locale.enum.danish.enabled=true
   bharosa.locale.enum.dutch.enabled=true
   bharosa.locale.enum.finnish.enabled=true
   bharosa.locale.enum.greek.enabled=true
   bharosa.locale.enum.hebrew.enabled=true
   bharosa.locale.enum.hungarian.enabled=true
   bharosa.locale.enum.norwegian.enabled=true
   bharosa.locale.enum.polish.enabled=true
   bharosa.locale.enum.portuguese.enabled=true
   bharosa.locale.enum.romanian.enabled=true
   bharosa.locale.enum.russian.enabled=true
   bharosa.locale.enum.slovak.enabled=true
   bharosa.locale.enum.swedish.enabled=true
   bharosa.locale.enum.thai.enabled=true
   bharosa.locale.enum.turkish.enabled=true
   ```

6. Set `bharosa.default.locale` property in `client_resource_`
   `<locale>.properties` to 9.

### F.3.3 Example 3

A French bank wants clients to see French as a default, and wants to support only
French, German, English, and Italian. The French locale enum is already present in the
`client_resource_fr.properties` file.

```
bharosa.locale.enum.french=5
bharosa.locale.enum.french.name=French
bharosa.locale.enum.french.description=French
bharosa.locale.enum.french.language=fr
bharosa.locale.enum.french.country=
bharosa.locale.enum.french.adminSupported=true
bharosa.locale.enum.french.enabled=true
```

To configure the application:

1. In `client_resource_fr.properties` set
   `bharosa.locale.enum.<locale>.enabled` to `true` for German, Italian, and
   English.

   ```
   bharosa.locale.enum.german.enabled=true
   bharosa.locale.enum.italian.enabled=true
   bharosa.locale.enum.english.enabled=true
   ```

2. Set all `other bharosa.local.enum.<locale>.enabled` properties to
   `false`.

3. Set `bharosa.default.locale` property to the value of the locale enum.

   Since `bharosa.locale.enum.french=5`, set `bharosa.default.locale`
   property to 5.

### F.3.4 Example 4

A German bank wants to set English as the default language and wants to support all
other languages. To do this, follow these steps for `client_resource_`
`de.properties`:

1. If the locale enum does not exist, create it:

   ```
   bharosa.locale.enum.english.enabled=true
   ```

2. If the locale enum already exists, set it to true.

3. If present, set other `bharosa.local.enum.<locale>.enabled` properties to
   true.

   ```
   bharosa.locale.enum.italian.enabled=true
   bharosa.locale.enum.german.enabled=true
   bharosa.locale.enum.french.enabled=true
   bharosa.locale.enum.portuguese_br.enabled=true
   bharosa.locale.enum.spanish.enabled=true
   bharosa.locale.enum.korean.enabled=true
   bharosa.locale.enum.chinese_cn.enabled=true
   bharosa.locale.enum.chinese_tw.enabled=true
   bharosa.locale.enum.japanese.enabled=true
   ```

```
bharosa.locale.enum.arabic.enabled=true
bharosa.locale.enum.czech.enabled=true
bharosa.locale.enum.danish.enabled=true
bharosa.locale.enum.dutch.enabled=true
bharosa.locale.enum.finnish.enabled=true
bharosa.locale.enum.greek.enabled=true
bharosa.locale.enum.hebrew.enabled=true
bharosa.locale.enum.hungarian.enabled=true
bharosa.locale.enum.norwegian.enabled=true
bharosa.locale.enum.polish.enabled=true
bharosa.locale.enum.portuguese.enabled=true
bharosa.locale.enum.romanian.enabled=true
bharosa.locale.enum.russian.enabled=true
bharosa.locale.enum.slovak.enabled=true
bharosa.locale.enum.swedish.enabled=true
bharosa.locale.enum.thai.enabled=true
bharosa.locale.enum.turkish.enabled=true
```

4. Set `bharosa.default.locale property` to match the value of the locale enum.

   Since `bharosa.locale.enum.english=0`, set `bharosa.default.locale` property to 0.

   If the property does not exist, create it.

## F.4 Dashboard

The Oracle Adaptive Access Manager Dashboard is an application that provides a high-level view of real monitor data. Monitor data is a representative sample of data. It presents a real-time view of activity via aggregates and trending.

To view the Dashboard in the language you want, set your browser's language preference to the appropriate language.

All data viewed in the Dashboard is based on the time zone of the server. This means that any data generated by OAAM is governed by the time zone of the server, and not the user time zone, but the information is presented per your browser settings. For information on setting the time zone, refer to Section 2.9, "Setting the Time Zone Used for All Time Stamps in the Administration Console."

For more information on the dashboard, refer to Chapter 24, "Using the Dashboard."

## F.5 Knowledge Based Authentication

Oracle Adaptive Access Manager provides out-of-the-box secondary authentication in the form of knowledge based authentication (KBA). KBA provides an infrastructure for challenge question creation and logic algorithm for registration and answers. This section contains information customizing certain KBA user experiences.

### F.5.1 Answer Logic Phonetics Algorithms

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

For information on customization, see Section 7.10, "Customizing English Abbreviations and Equivalences."

The phonetics algorithm is only supported in English.

For information on customization for locales, see Section 7.11, "Customizing Abbreviations and Equivalences for Locales."

## F.5.2 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 the fat fingering algorithm.

The fat fingering algorithm is only supported in English.

## F.5.3 Adding Abbreviations and Equivalences for Answer Logic

Oracle Adaptive Access Manager supports the concept of "fuzzy logic." Fuzzy logic, in part, relies on pre-configured sets of word equivalents, commonly known as abbreviations.

In the English version of Oracle Adaptive Access Manager, there are several thousand English abbreviations (and equivalences).

In all other languages, it is necessary for the installer to enhance the brief abbreviation files provided. Without additions, the fuzzy logic will be not as effective.

For information on customizing abbreviations and equivalences for locales, refer to Section 7.11, "Customizing Abbreviations and Equivalences for Locales."

## F.5.4 Adding Registration Questions

The deployment administrator must ensure that there are enough questions in the database for each of the supported locale as configured in OAAM Admin during deployment; otherwise, OAAM Server displays only the English language questions during registration.

The number of locale-specific questions must be equal to or greater than the "Questions User Will Register" multiplied by the "Questions per Menu" multiplied by the "Categories per Menu."

For information on adding registration questions, refer to Section 7.5.3, "Creating a New Question."

# G

# Oracle Adaptive Access Manager Properties

This appendix provides essential properties used by Oracle Adaptive Access Manager.

## G.1 Properties

**Action Override**

The Action Override feature is turned off by default. To enable action overrides, set the following property to "true":

```
vcrypt.tracker.rules.allowControlledActions
```

**Authenticator Phrase**

To customize the phrase in the virtual authentication device, set the following two parameters:

```
bharosa.user.noun.list
bharosa.user.adj.list
```

The authenticator phrase is created by these two properties.

Both are comma-separated lists of words.

Examples:

```
actors,age,air,aircraft
abundant,accessible,accommodating
```

For images to be displayed, set the following properties

```
vcrypt.user.image.dirlist.property.name=bharosa.image.dirlist
bharosa.image.dirlist=<imagePath>
```

The following property in `client_resource_<locale>.properties` determines whether the QuestionPad is set for visible text input or password (non-visible) input.

```
bharosa.authentipad.questionpad.datafield.input.type
```

Valid values are text and password.

The accessible versions of the pads contain tabbing, directions and ALT text necessary for navigation via screen reader and other assistive technologies.

To enable these versions, set the is ADA compliant flag to true.

For native integration the property to control the pads is

```
desertref.authentipad.isADACompliant
```

For UIO, the property to control the pads is

```
bharosa.uio.default.authentipad.is_ada_compliant
```

**Autolearning**

To enable autolearning properties:

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 autolearning.

2.  Set the following properties to true:

    -   `vcrypt.tracker.autolearning.use.auth.status.for.analysis`

        This property must be set to true for the authentication patterns to work. Authentication patterns are the patterns that analyze the data related to authentication (login) related information only.

    -   `vcrypt.tracker.autolearning.use.tran.status.for.analysis`

        This property must be set to true.

3.  If the properties do not exist, create them.

**User Name in Lowercase**

If you want the user name to be in lowercase, set `bharosa.uio.default.username.case.sensitive` to false.

By default this property is set to true.

When it is set to true, the user name is always in lower case. If it is set to false, the user name is taken as is.

For example:

```
myusername
```

```
MyUserName
```

```
myUserName
```

If property is true (default), all of these are the same user and will appear in OAAM Admin as "myusername".

If property is false, all of these are different users and will appear in OAAM Admin as entered.

**Configurable Actions**

To enable the configurable actions feature, set `dynamicactions.enabled` to true.

**Device Registration**

Setting the following properties adds text and a checkbox to the bottom of the challenge page. When a user is challenged, the checkbox and text would allow him to register the current device (if it is not already registered). If the device is already registered for that user, the option will not appear unless the user unregisters the device in user preferences.

```
bharosa.uio.default.registerdevice.enabled=true
bharosa.uio.default.userpreferences.unregister.this.enabled=true
```

```
bharosa.uio.default.userpreferences.unregister.all.enabled=true
```

In native integration, to enable device registration:

Set bharosa.tracker.send.devideId to true, so the device ID can be captured

### Enumerations

For the enumerations to be listed in the Properties Editor, you must set the following property to false:

```
bharosa.config.ui.list.filter.enum=false
```

### Expiry Behavior for CSR Cases

To set "expiry" behavior for CSR cases (default setting), modify the following properties:

```
customercare.case.expirybehavior.enum.csrcase.behavior = expiry
customercare.case.expirybehavior.enum.csrcase.label = Expired
customercare.case.expirybehavior.enum.csrcase.durationInHrs = 24
customercare.case.expirybehavior.enum.csrcase.resetonaccess = false
```

When durationInHrs is set to 24 hours, the case expires in a day.

When resetonaccess is set to true, the expiration date is reset when a case is accessed.

To disable the "expiry" behavior for CSR cases, modify the following property:

```
customercare.case.expirybehavior.enum.csrcase.behavior = none
```

### KBA

Ensure the `bharosa.kba.active` property is set to true.

The "Questions user will register" setting should be between 3 and 7. 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.

The max and min limits are configurable through the following properties.

```
bharosa.config.type.kba_config.enum.regQuestionsCount.validation.minValue=3
bharosa.config.type.kba_config.enum.regQuestionsCount.validation.maxValue=7
```

### Proxy Mode Setting

OAAM Server is configured to be in non-proxy mode with the flag `bharosa.uio.proxy.mode.flag` set to false by default.

The user must explicitly configure OAAM Server to be used in proxy mode.

### Scheduler

To enable scheduler so that jobs are run, set the following property to true:

```
vcrypt.reports.scheduler.activate
```

By default, the property is set to false. Jobs can be created, but they will not run until the property is changed to true.

### Transactions in Session Details

Before you can view transactions in the Session Details page, you must set the property to show transactions to true.

```
bharosa.trackeradmin.show.transaction.detail=true
```

Setting the property to false turns off the display for transactions.

## G.2  Time Zone

A time zone identifies an area that always shares the same local time.

To set the time zone that will be used for all timestamps in the user interface, use the Property Editor to set `oaam.adf.timezone` to the desired time zone.

For example,

`oaam.adf.timezone = Atlantic/Reykjavik`

# H

# Device Fingerprinting

Oracle Adaptive Access Manager contains proprietary clientless technologies for fingerprinting and interrogating devices used during access requests and transactions. Device fingerprinting is a mechanism to recognize the devices a customer uses whether it is a desktop computer, laptop computer or other web-enabled device. This appendix contains details about device fingerprinting.

## H.1 What is Device Fingerprinting

Oracle Adaptive Access Manager device fingerprinting is a capability used to recognize the devices a user uses to login and conduct transactions. It collects information about the device like browser type, browser headers, operating system type, locale, and so on. Fingerprint data represents the data collected for a device during login process required to identify the device whenever it logs in the next time. The fingerprint details help in identifying whether a device is secure and determine the risk level of the authentication or transaction.

A device is identified using proprietary logic and a set of specialized policies to process available data and arrive at identification. The intelligent identification does not rely on any single attribute type so it can function on user devices not following strict specifications and in both web and non-web channels. The device identification is not merely a static list of attributes but is instead a dynamic capture, evaluation and profiling of the specific combinations of attributes available in each access request or transaction. This is especially important in large consumer facing deployments.

## H.2 When is a Device Fingerprinted

The fingerprinting process can be run any number of times during a user session to allow detection of changes mid-session that can indicate session hijacking. OAAM monitors a comprehensive list of device attributes. If any attributes are not available the device can still be fingerprinted. The single-use capabilities combined with server-side logic defends against the fingerprint being stolen and reused on another machine to commit fraud.

## H.3 Device Fingerprint Attributes

Device fingerprinting collects information about the device such as browser type, browser headers, operating system type, locale, and so on. The fingerprint details can help in identifying a device, check whether it is secure, and determine the risk level for the authentication or transaction.

### H.3.1 Browser Characteristics

Browser fingerprinting gathers information that include the browser type used, plug-ins installed, system fonts, and the configuration and version information from the operating system, and whether or not the computer accepts cookies.

### H.3.2 Device Characteristics

Flash fingerprinting is similar to browser fingerprinting but a flash movie is used by the server to set or retrieve a cookie from the user's machine so a specific set of information is collected from the browser and from flash. The flash fingerprint is only information if flash is installed on the client machine.

**I**

# Setting Up Archive and Purge Procedures

Archiving is the process of backing up the obsolete data that will be deleted during the purge process. During the archive process, data will be moved from the main transactional tables to the backup tables. By default the Oracle Adaptive Access Manager purge scripts will archive data that will be deleted during the purge process.

Purging is the process of freeing up space in the database or of deleting obsolete data that is not required by the system. The purge process can be based on the age of the data or the type of data.

This chapter describes how to archive and purge data from the OAAM database using SQL scripts.

A DBA or system administrator, who performs routine maintenance and the archiving and purging of the Oracle Adaptive Access Manager database, should follow the instructions in this chapter.

This chapter contains the following sections:

- Overview
- Setting Up the Scripts in Database
- Best Practices/Guidelines for Running Purge Scripts
- Running the Scripts
- Validating Archive and Purge
- Restoring Archived Data
- Running Partition Maintenance Scripts
- Details of Data that is Archived and Purged
- Archive and Purge Criteria
- List of Related Stored Procedures

## I.1 Overview

The archive and purge process allows the releasing of data that is not required anymore for rules evaluation or fraud investigation.

- Archiving is the process of moving data from main transactional tables to the archive tables.
- Purging is the process of deleting obsolete data that is not required by the system.

  Not all the tables are purged since many of them do not have data growth issues.

"Purging data" is different from "backing up data". A data backup is for the recovery of data if loss occurs; purges are for keeping the runtime tables free of old data. Regardless, to protect your data, database backups should be performed on a regular basis with the help of a database administrator.

The following data can be archived or purged using the scripts provided in the archive `IDM_ORACLE_HOME/oaam/oaam_db_scripts/oaam_db_purging_scripts.zip`:

- Login and devices data

- Rule Logs data

- Auto Learning data

- Transactions and Entities data

- Profile data

Archive and purge criteria is based on the create/update timestamp of the records. This is specified using the retention period described using number of days.

The following is the overview of the archive and purge process:

1. Determine the retention period (usually 180 days; that is 6 months)

2. Determine whether to purge or archive.

3. Deploy the purge related stored procedures into the OAAM database. This is a one-time job.

4. Determine what types of data have to be archived and purged.

5. Schedule the related scripts to run on regular intervals or manually run the scripts when required.

6. Check for entries where the `LOG_TYPE` is `99` in the database table `V_SYS_LOGS`.

The next sections describe the above in detail.

## I.2 Setting Up the Scripts in Database

To archive and purge OAAM data, you must set up the one-time scripts.

1. Create a scripts directory `oaam_purge_script`.

2. Unzip the scripts archive `IDM_ORACLE_HOME/oaam/oaam_db_scripts/oaam_db_purging_scripts.zip` to the scripts directory.

3. Log in to the database using the `sys` or `sysdba` account.

4. Grant the following privileges to the OAAM schema so that stored procedures can be created and executed:

   ```
   GRANT create any procedure TO <schema_name>;

   GRANT create any table TO <schema_name>;

   GRANT create any index TO <schema name>;

   GRANT create procedure TO <schema_name>;

   GRANT execute any procedure TO <schema_name>;
   ```

5. Now connect to the OAAM schema using the OAAM user name and password. For example:

   ```
   sqlplus <oaam_db_user_name>/<oaam_db_password>
   ```

6. Run the `create_purge_proc.sql` script

   `SQL> @oracle_db/create_purge_proc.sql`

7. Validate the stored procedures to make sure they are valid and without errors.

> **Note:** The purging/archiving scripts need the CREATE Any privilege to create and execute purge related stored procedures.
>
> Since the purging/archiving scripts use custom rebuild index stored procedures for a given table, this stored procedure requires `CREATE Any Table` and `Create Any index` privileges granted to the Oracle Adaptive Access Manager schema. If these privileges are not granted, the `rebuild_oaam_index` stored procedure will not work.
>
> These privileges must be granted to set up and execute the Oracle Adaptive Access Manager purging/archiving routines and must be revoked after the purging/archiving process is completed.

## I.3 Best Practices/Guidelines for Running Purge Scripts

Best/practices guidelines for running purge scripts are as follows:

- Determine the retention period based on the business requirements and rules and policies used

- Perform regular purge/archive

- Make sure replication is not enabled during the window when these scripts are run

- Run these during off peak load hours which Oracle recommends you do. Archive and purge could be resource (like CPU) intensive.

- If archiving is required, make sure there is enough disk space available on the database server since the data would be moved to archive tables instead of simply purging. Archival space should be equal to or greater than the current table's storage.

- Plan your purging strategy since purging requires a significant amount of time if there are millions of rows that need to be deleted or copied from the database.

- In a multi-data center, it is recommended that you run purges at low data flow since the data in tables is replicated. You should consult your database administrator if you have multidimensional clustering (MDC) set up and require purging.

- Oracle recommends that custom purging scripts only include the tables used by the standard purging scripts provided. The alterations to the provided purge scripts can include parameterization for user ID. Such alterations should be thoroughly tested before being used in production to ensure they function as expected.

## I.4 Running the Scripts

To run the archive and purge scripts, proceed as follows:

1. Set the `p_days1` and `p_archived` parameters. All the scripts have these two parameters that you can set. Table I–1 describes these parameters.

*Table I–1   Archive and Purge Routine Parameters*

| Variable Name | Default Value | Description |
|---|---|---|
| p_days1 | 180 | Retention period in days. Data older than this many number of days will be archived or purged. |
| p_archived | Y | Y or N for Yes and No respectively. If "Y" then data will be archived (in archive tables), otherwise data will be purged based on the retention period. |

2. Select the scripts to run based on the data that has to be archived or purged. Table I–2 lists the types of data and corresponding script name.

*Table I–2   Archive and Purge Scripts Based on Types of Data*

| Type of Data | Corresponding Script |
|---|---|
| Login, Device Data | exec_sp_purge_tracker_data.sql |
| Rules, Policy Log Data | exec_sp_purge_rule_log.sql |
| Transactions, Entities Data | exec_sp_purge_txn_log.sql |
| Autolearning Data | exec_sp_purge_workflow_data.sql |
| Profile Data | exec_sp_purge_profile_data.sql |
| Cases related Data | exec_sp_purge_case_data.sql |
| Monitor Data | exec_v_monitor_purge_proc.sql |

3. Log in to the OAAM database using OAAM database user name and password and execute the selected scripts.

4. Check the corresponding log file and see if there are any errors or warnings.

5. If archiving is selected, then make sure to take a backup of the archive tables so that data can be restored if needed.

### Registration of Safe Devices

The OAAM purge/archive process does not remove registration of "safe" devices and cause users to have to re-register safe devices unless the device has not been used for six months.

Purge scripts unregister the devices when the devices are purged as part of tracker_purge_job.sql). As part of tracker_purge_job.sql, all the unused devices (that are not referred by any record in VCRYPT_TRACKER_USERNODE_LOGS) are purged and also the related records in VT_USER_DEVICE_MAP are purged.

### Automatic Scheduling

Archive and purge jobs should be part of a routine schedule. These jobs can be scheduled using database jobs or OS-based scheduling utilities (`crontab`, `at`) or scheduler software (`autosys`, `appworx`).

It is recommended that these scripts are scheduled to run on regular intervals and only during off-peak hours.

## I.5 Validating Archive and Purge

To determine if the archive and purge was successful, check the log files (for example scheduler log, script output log, and others) for any errors. When the archive and purge process has completed, users can also query the transactional log and its related purged tables to validate that the data was archived and purged.

## I.6 Restoring Archived Data

As recommended, users should take an export backup of archived tables after the archive process has completed in case they should need to perform troubleshooting in the future.

When performing a restoration, the user should restore the desired date's data to a temporary table using Oracle's database Import feature.

Contact Oracle Support Services if any data restoration is required.

## I.7 Running Partition Maintenance Scripts

In case the partitioned version of OAAM database is used, there are related scripts to drop the partitions.

### I.7.1 Dropping Weekly Partitions

To drop weekly partitions, proceed as follows:

1. Run this script at the end of every two weeks starting from your database creation date.

2. To change the default retention period, open the script `Drop_Weekly_Partition_tables.sql` and set the retention period in days. Default is set to `15` days (two weeks).

3. Log in to the OAAM database using the OAAM database user name and password.

4. Execute the script `Drop_Weekly_Partition_tables.sql`.

### I.7.2 Dropping Monthly Partitions

To drop monthly partitions, proceed as follows:

1. Run this script at the end of each month to drop partitions that are older than the sixth month.

2. To change the default retention period, open the script `Drop_Monthly_Partition_tables.sql` and set the retention period in days. Default is set to `180` days (6 months).

3. Log in to the OAAM database using the OAAM database user name and password.

4. Execute the script `Drop_Monthly_Partition_tables.sql`.

## I.8 Details of Data that is Archived and Purged

Details of data that is purged and the corresponding archived tables are presented in the following sections.

## I.8.1 Login and Device Data

*Table I–3    Login and Device*

| Login and Device Tables | Corresponding Archived Tables |
| --- | --- |
| VCRYPT_TRACKER_NODE | VCRYPT_TRACKER_NODE_PURGE |
| VCRYPT_TRACKER_NODE_HISTORY | VCRYPT_TRACKER_NODE_HISTORY_PURGE |
| VCRYPT_TRACKER_USERNODE_LOGS | VCRYPT_TRACKER_USERNODE_LOGS_PURGE |
| VT_DYN_ACT_EXEC_LOG | VT_DYN_ACT_EXEC_LOG_PURGE |
| VT_SESSION_ACTION_MAP | VT_SESSION_ACTION_MAP_PURGE |
| VT_USER_DEVICE_MAP | VT_USER_DEVICE_MAP_PURGE |

> **Note:**  The VT_SESSION_ACTION_MAP table is not purged using the partition drop maintenance script. This table stores the device fingerprinting session information; therefore the purging of this table is performed using the manual purge stored procedure (`SP_SESS_ACT_MAP_PROC`) which is called by the `exec_sp_purge_tracker_data.sql` script.

## I.8.2 Rules and Policy Log Data

*Table I–4    Rules and Policy Log Data Tables*

| Rules, Policy Log Tables | Corresponding Archived Tables |
| --- | --- |
| VR_POLICYSET_LOGS | VR_POLICYSET_LOGS_PURGE |
| VR_RULE_LOGS | VR_RULE_LOGS_PURGE |
| VR_MODEL_LOGS | VR_MODEL_LOGS_PURGE |
| VR_POLICY_LOGS | VR_POLICY_LOGS_PURGE |

## I.8.3 Transactions and Entities Data

*Table I–5    Transactions and Entity Data Tables*

| Transaction Tables | Corresponding Archived Tables |
| --- | --- |
| VT_ENTITY_ONE | VT_ENTITY_ONE_PURGE |
| VT_ENTITY_ONE_PROFILE | VT_ENTITY_ONE_PROFILE_PURGE |
| VT_USER_ENTITY1_MAP | VT_USER_ENTITY1_MAP_PURGE |
| VT_ENT_TRX_MAP | VT_ENT_TRX_MAP_PURGE |
| VT_TRX_DATA | VT_TRX_DATA_PURGE |
| VT_TRX_LOGS | VT_TRX_LOGS_PURGE |

## I.8.4  Autolearning Data

*Table I–6    Autolearning Data Tables*

| Autolearning Transactional Tables | Corresponding Archived Tables |
| --- | --- |
| VT_WF_DAYS | VT_WF_DAYS_PURGE |
| VT_WF_HOURS | VT_WF_HOURS_PURGE |
| VT_WF_MONTHS | VT_WF_MONTHS_PURGE |
| VT_WF_YEARS | VT_WF_YEARS_PURGE |
| V_FPRINTS | V_FPRINTS_PURGE |
| V_FP_MAP | V_FP_MAP_PURGE |

## I.8.5  Profile Data

*Table I–7    Profile Data Tables*

| Transactional Tables | Corresponding Archived Tables |
| --- | --- |
| VT_USER_PROFILE | VT_USER_PROFILE_PURGE |
| VT_DEVICE_PROFILE | VT_DEVICE_PROFILE_PURGE |
| VT_BASE_IP_PROFILE | VT_BASE_IP_PROFILE_PURGE |
| VT_IP_PROFILE | VT_IP_PROFILE_PURGE |
| VT_STATE_PROFILE | VT_STATE_PROFILE_PURGE |
| VT_CITY_PROFILE | VT_CITY_PROFILE_PURGE |
| VT_COUNTRY_PROFILE | VT_COUNTRY_PROFILE_PURGE |

## I.8.6  Cases-Related Data

*Table I–8    Case-Related Data Tables*

| Transaction Tables | Corresponding Archived Tables |
| --- | --- |
| V_CASE | V_CASE_PURGE |
| V_CASE_HIST | V_CASE_HIST _PURGE |
| V_ACTION_LOG_SESS_MAP | V_ACTION_LOG_SESS_MAP_PURGE |
| V_ACTION_LOG_SESS | V_ACTION_LOG_SESS |
| V_CASE_MAP | V_CASE_MAP_PURGE |
| V_CASE_MAP_HIST | V_CASE_MAP_HIST_PURGE |

## I.8.7  Monitor Data

*Table I–9    Monitor Data Tables*

| Transaction Table | Corresponding Archived Table |
| --- | --- |
| V_MONITOR_DATA | V_MONITOR_DATA_PURGE |

## I.9  Archive and Purge Criteria

Archive and purge criteria is presented in the following table.

*Table I–10    Archive and Purge Criteria*

| Type of Data | Purge Criteria |
| --- | --- |
| Device Fingerprinting Data | The purge process archives and purges device fingerprinting data based on the following criteria:<br><br>■ Device fingerprinting logs that are older than a specified period first.<br><br>■ User device maps that are not used after the data from the device fingerprinting logs<br><br>■ Device history that is not used after the data from the device fingerprinting logs<br><br>■ Device data that is not used after the data from the device fingerprinting logs |
| Transaction In-Session Based Data | The purge process archives and purges in-session transaction data based on the following criteria:<br><br>■ In-session transactional-based data that is older than a specified period first<br><br>■ Transaction data that is not used in the transaction data after the transactions logs are purged for a specific time period<br><br>■ Entity, entity profile, user entity map and entity transaction map after the transactions logs are purged for a specific time period |

*Table I–10   (Cont.)  Archive and Purge Criteria*

| Type of Data | Purge Criteria |
| --- | --- |
| Autolearning Profile Data | Archive and purge the following tables based on a specific time period. |
| | ■ HOURS based tables will retain 3 days worth of data. |
| | ■ DAYS based tables will retain 32 days worth of data. |
| | ■ MONTHS based tables will retain 1 years worth of data. |
| | ■ YEARS based tables will retain 5 years worth of data. |
| | Archive and purge fingerprint data for AUTH and TRANSACTION fingerprint types. Fingerprint data to be purged in this way is in fingerprint table and fp_map table. HOURS, DAYS, MONTHS, and YEARS tables described above also have references to fingerprint. Before purging fingerprint data, make sure that archiving and purging of HOURS, DAYS, MONTHS, and YEARS tables is performed. |
| | `vcrypt.fingerprint.type.enum.autolearning.auth=11`<br>`vcrypt.fingerprint.type.enum.autolearning.transaction=12` |
| | 11 is the enumeration value for the autolearning AUTH type. Change these values in the script if another value was used during integration. |
| | 12 is enumeration value for the autolearning TRANSACTION type. Change these values in the script if another value was used during integration. |
| Rule Log Data | The rule log transaction data that is 30 days old is archived and purged. |
| | This retention value should be set based on the customer care requirements. If the reporting database is used, then, rule logging data retention should be less than 30 days. |
| Registration of Safe Devices | The OAAM purge/archive process does not remove registration of "safe" devices and cause users to have to re-register safe devices unless the device has not been used for six months. |
| | Purge scripts unregister the devices when the devices are purged (as part of tracker_purge_job.sql). As part of tracker_purge_job.sql, all the unused devices (that are not referred by any record in VCRYPT_TRACKER_USERNODE_LOGS) are purged and also the related records in VT_USER_DEVICE_MAP are purged. |

## I.9.1  Minimum Data Retention Policy

Based on the Oracle Adaptive Access Manager system requirement, the minimum data retention policy for various OLTP tables are shown below, but users should determine the data retention period based on their business requirements. For more information, review the information in this chapter.

### I.9.1.1  Device Fingerprinting Data

Minimum of 6 months or 180 days

### I.9.1.2  In-session Transactional Tables

Minimum of 6 months or 180 days

### I.9.1.3  Auto-learning and Workflow Tables

■ HOURS based Workflow tables will retain 3 days' worth of data.

■ DAYS based Workflow tables will retain 32 days' worth of data.

- MONTHS based Workflow tables will retain 1 year's worth of data.

- YEARS based Workflow tables will retain 5-years' worth of data.

### I.9.1.4 Rule Log Data

The script will archive and purge all rule log data that is 30 days older (This value should be set based on the customer care requirement. If the reporting database is used, then, rule logging data retention should be less than 30 days.

# I.10 List of Related Stored Procedures

The archive and purge setup scripts for the Oracle Database are listed in this subsection.

## I.10.1 create_purge_proc.sql

The `create_purge_proc.sql` script creates the following stored procedures to archive and purge data from the transaction tables:

- SP_RULE_ PROC

- SP_MODEL_ PROC

- SP_POLICYSET_ PROC

- SP_POLICY_ PROC

- SP_NODE_HISTORY_ PROC

- SP_NODE_PROC

- SP_USER_NODE_PROC

- SP_USER_DVC_PROC

- SP_SESS_ACT_MAP_PROC

- SP_WF_YEARS_PROC

- SP_WF_MONTHS_PROC

- SP_WF_DAYS_PROC

- SP_WF_HOURS_PROC

- SP_V_FPRINTS_PROC

- SP_V_FP_MAP_PROC

- SP_VT_DY_ACT_EX_LOG_PRO

- SP_VT_TRX_LOGS_PROC

- SP_VT_TRX_DATA_PROC

- SP_VT_ENT_TRX_MAP_PROC

- SP_VT_ENT_ONE_PRF_PROC

- SP_VT_ENT_ONE_PROC

- SP_VT_ENT_ONE_MAP_PROC

- SP_VT_USER_PRF_PROC

- SP_VT_DEVICE_PRF_PROC

- SP_VT_IP_PRF_PROC
- SP_VT_BASE_IP_PRF_PROC
- SP_VT_CITY_PRF_PROC
- SP_VT_COUNTRY_PRF_PROC
- SP_VT_STATE_PRF_PROC

## I.10.2 create_case_purge_proc.sql

The create_case_purge_proc.sql script creates the following stored procedures to archive and purge data from the transaction tables:

- SP_V_CASE_PROC
- SP_V_CASE_HIST_PROC
- SP_V_CASE_MAP_PROC
- SP_V_CASE_MAP_HIST_PROC
- SP_V_ACTION_LOG_SESS_MAP_PROC
- SP_V_ACTION_LOG_SESS_PROC

## I.10.3 create_v_monitor_purge_proc.sql

The create_v_monitor_purge_proc.sql script creates the following stored procedure, SP_V_MON_DATA_PURGE_PROC, to archive and purge data from the transaction table.

# J

# Configuring SOAP Web Services Access

This appendix presents instructions on configuring SOAP Web services access.

## J.1 Web Services Access

Web services let you access Oracle Adaptive Access Manager functionality that is made available on a remote computer. The OAAM web service enables you to make a request to OAAM to perform an action.

The advantage the OAAM web services is that you do not have to recreate application logic that has already been created.

Referencing a remote web service within your application is called consuming web services. You can consume a web service implemented as part of a .NET or Java application.

## J.2 Requirements

The requirements for accessing the OAAM web service are the following:

- Configuration of the SOAP web access requires the OAAM Extensions Shared Library for Native Integration using SOAP

- The configurable properties must be specified in `bharosa_server.properties` and this file should be in the Java Classpath of the client application.

## J.3 OAAM Server Side Setup

An access to a web service is similar to a function call except it references remote functionality over the Internet instead of referencing a library on your computer.

SOAP provides a standard XML structure for sending and receiving web service requests and responses over the Internet. The SOAP messages are sent using HTTP.

Web Services/SOAP clients need to send the username and password for successful communication with OAAM web services.

The password needs to be stored in a KeyStore for security.

Making web services available to others for remote access is called publishing web service.

Out-of-the-box, OAAM publishes Web services at the URL: /oaam_server/services. This URL is secured by HTTP authentication.

Access to this URL is allowed to the users with the OAAMSOAPServicesGroup role/group. You must add a user (a.k.a SOAP User) with the OAAMSOAPServicesGroup role/group to the OAAM Domain.

> **Note:** This step is not required if SOAP Authentication is disabled on the OAAM server

## J.4 Client Side Setup

The client side setup is documented below.

### J.4.1 Setup Client Keystore with Password of the SOAP User

To set up security for Native Client web services:

1. In the *$ORACLE_HOME*/oaam/cli directory, create a file, for example, `soap_key.file`, and enter the HTTP authentication user password in it. (The password from the user that was added to the OAAMSOAPServicesGroup role/group).

2. Copy `sample.config_3des_input.properties` to `soap_3des_input.properties`.

   ```
   cp sample.config_3des_input.properties soap_3des_input.properties
   ```

3. Update `soap_3des_input.properties` with the keystore password, the alias password, and password file.

   ```
   #This is the password for opening the keystore.
   keystorepasswd=

   #This is the password reading alias (key) in the keystore
   keystorealiaspasswd=

   #File containing from key. Please note, keys in AES could be binary. Also note
   algorithms like 3DES require minimum 24 characters in the key
   #keyFile=soap_key.file
   keyFile=
   ```

4. Set `ORACLE_MW_HOME` and `JAVA_HOME` and source `setCliEnv.sh`.

5. Generate the keystore.

   - For Unix/Linux, run

     ```
     $JAVA_EXE -Djava.security.policy=conf/jmx.policy -classpath $CLSPTH
     com.bharosa.vcrypt.common.util.KeyStoreUtil updateOrCreateKeyStore
     readFromFile=soap_3des_input.properties
     ```

   - For Windows, run

     ```
     genkeystore.cmd soap_3des_input.properties
     ```

   If the `KeyStore` command was successful, you will see output similar to the following:

   ```
   updateOrCreateKeyStore done!
   Keystore file:system_soap.keystore,algorithm=DESede
   KeyStore Password=ZG92ZTEyMzQ=
   Alias Password=ZG92ZTEyMw==
   ```

6. Note down the Keystore password and Alias Password print on the screen. You will need to add these to `bharosa_server.properties`.

7. Save the system_soap.keystore file in your source code control system. Please take adequate security precaution while handling this file. The file contains critical password information. Make sure that only authorized personnel have read access to this file. If you lose it, Oracle Adaptive Access Manager will not be able to recover data encrypted.

8. Copy system_soap.keystore to the classpath of the Native Client deployment folder.

9. Delete both the `soap_key.file` and `soap_3des_input.properties` files.

10. Add the following properties with the encoded passwords (from step 5) and the authentication username to `bharosa_server.properties`.

```
vcrypt.soap.auth.keystorePassword=<base64 encoded keystore password>
vcrypt.soap.auth.aliasPassword=<based64 encoded password to the alias>
vcrypt.soap.auth.username=<user configured for accessing the soap services>
vcrypt.soap.auth.keystoreFile=system_soap.keystore
```

Note: This step is not required if SOAP Authentication is disabled on the OAAM server.

See "Disable SOAP Authentication" section for details on disabling authentication from client side.

## J.4.2  Disable SOAP Authentication

To disable or enable, HTTP authentication for Adaptive Strong Authenticator, set the following property to true (enabled) or false (disabled).

```
vcrypt.soap.auth=
```

## J.4.3  Specify SOAP Class

Set the vcrypt.common.util.vcryptsoap.impl.classname property.

This setting specifies for the application which libraries to use when creating SOAP messages to exchange with the OAAM services.

The available option is:

```
com.bharosa.vcrypt.common.impl.VCryptSOAPGenericImpl
```

## J.4.4  Specify SOAP Server Side URL

Set the `vcrypt.tracker.soap.url` property.

For example,

```
vcrypt.tracker.soap.url=http://localhost:14300/oaam_server/services/
```

This setting is the location of the web services with which the application will communicate.

## J.4.5  Specify SOAP Call Timeout

Set the `vcrypt.soap.call.timeout` property in milliseconds.

For example,

```
vcrypt.soap.call.timeout=10000
```

## J.5  Disabling SOAP Service Authentication on the Server

You can enable or disable authentication using Oracle Web Services Manager (OWSM) policies through Oracle Enterprise Manager Fusion Middleware Control.

If you disable the SOAP Web Service authentication on the server (which is by default enabled), the client can use the web service without having been authenticated.

1. Log in to Oracle Enterprise Manager Fusion Middleware Control of the Identity Management domain using the URL `http://<host-name>:7001/em` and WebLogic Admin user name and password.

2. Locate **oaam_server_server1** in the left hand side menu by expanding **WebLogic Domain** and the OAAM domain under it.

3. Right click the **oaam_server_server1** and select the **Web Services** menu option.

4. Click the **Oracle Infrastructure Web Services** tab.

5. Click the **Attach Policies** link in the top-right area of the page.

6. Select all the rows related to the OAAM Web services in the next page and click the **Next** button.

7. Select the rows **oracle/no_authentication_service_policy** and **oracle/no_authorization_service_policy** and click the **Next** button.

8. Click the **Attach** button in the next page.

9. Restart OAAM Server if required.

# K

# Configuring Logging

Logging is the mechanism by which components write messages to a file.

Oracle Adaptive Access Manager 11*g* components use the package java.util.logging as part of its logging infrastructure. This package is available in all Java environments.

> **Note:** On a production machine, you want to manage the amount of time logging is enabled since increasing the amount of logging may negatively affect performance.

## K.1 Logging Configuration File

Logging is initialized using the default logging configuration file, `logging.properties`, that is read at startup.

The file is located in the Home directory. It configures the Oracle Adaptive Access Manager Framework loggers to print messages. Through editing this file, you can:

- Specify the level of detail in the log messages.

- Specify whether log messages are sent to the console, to a file or to both

- Specify logging at the level of individual areas for which a logger is defined

## K.2 Oracle Adaptive Access Manager Loggers

The OAAM loggers generate logging messages to report on errors, provide additional information about OAAM. Oracle Adaptive Access Manager Loggers are described in Table K–1.

*Table K–1   Oracle Adaptive Access Manager Loggers*

| Logger | Components |
| --- | --- |
| oracle.oaam.model | ADF Models package, all classes with package starting with oracle.oaam.model |
| oracle.oaam.view | ADF View package, all classes with package starting with oracle.oaam.view |
| oracle.oaam.alerts | Alerts, rules engine specifically uses this logger so that custom handlers can consume these log records |
| oracle.oaam | root Logger controls all oaam logging |

## K.3 Logging Levels

The log levels define the importance and urgency of a log message. The class Level is used to define which messages should be written to the log. Log messages have an associated log level. Logging levels in descending order are listed below.

*Table K–2 Logging Levels*

| Level | Description |
|---|---|
| SEVERE | The highest value; intended for extremely important messages (e.g. fatal program errors). SEVERE is used to diagnose if there is improper functioning of the system. |
| WARNING | Intended for warning messages. |
| INFO | Informational runtime messages. Any logging at INFO and above provides complete details. Any logging message below INFO should have its logging enabled to check for performance reasons (isDebugEnabled() / isLevelEnabled()). |
| CONFIG | Informational messages about configuration settings/setup. |
| FINE | Used for greater detail, when debugging/diagnosing problems. |
| FINER | Even greater detail. |
| FINEST | The lowest value; greatest detail. |
| ALL | Enables logging of all records |
| OFF | Used to turn off logging |

**Property to Control Logging Level**

The following property controls the level of logging:

```
Logger Name=Level
```

**Enable Debug Log**

Example, to enable debug logs:

```
oracle.oaam.level=FINER
```

**Enable Debug Logs for ADF Models**

To enable debug logs for ADF models package and reset all information logging, the following entries may be added:

```
oracle.oaam.level=INFO
oracle.oaam.model.level=FINER
```

**Configure all logs to use FINER logging (include debug)**

To configure oracle.oaam to use FINER logging (include debug)

```
oracle.oaam.level=FINER
```

## K.4 Handlers

Each logger has access to handlers. The handler receives the log message from the logger and output the log messages to a file or to both.

Appendix K–3 shows the handlers used by Oracle Adaptive Access Manager

*Table K–3   Handler Classes*

| Handler Class | Function |
| --- | --- |
| FileHandler | Writes formatted log records either to a single file, or to a set of rotating log files. |
| ConsoleHandler | Writes formatted records to System.err |

### K.4.1  Configuring the File Handler

To send logs to a file, add FileHandler to the handlers property in the `logging.properties` file. This will enable file logging globally.

```
handlers= java.util.logging.FileHandler
```

Configure the handler by setting the following properties:

```
java.util.logging.FileHandler.pattern=<home directory>/logs/oaam.log
java.util.logging.FileHandler.limit=50000
java.util.logging.FileHandler.count=1
java.util.logging.FileHandler.formatter=java.util.logging.SimpleFormatter
```

**java.util.logging.FileHandler.pattern** specifies the location and pattern of the output file. The default setting is your home directory.

**java.util.logging.FileHandler.limit** specifies, in bytes, the maximum amount that the logger writes to any one file.

**java.util.logging.FileHandler.count** specifies how many output files to cycle through.

**java.util.logging.FileHandler.formatter** specifies the java.util.logging formatter class that the file handler class uses to format the log messages. SimpleFormatter writes brief "human-readable" summaries of log records.

### K.4.2  Configuring Both Console Logging and File Logging

You can set logging to output log messages to both the console and to a file by specifying the console handler and the file handler, separated by a comma, as shown:

```
handlers= java.util.logging.FileHandler, java.util.logging.ConsoleHandler
```

## K.5  Redirecting oracle.oaam Logs

To redirect oracle.oaam logs to file handler (oaam.log), set the following property:

```
oracle.oaam.handlers=java.util.logging.FileHandler
```

If you want logs to go to both console and file, comment the following property:

```
oracle.oaam.useParentHandlers=false
```

To instruct java to use this configuration file instead of *$JDK_ HOME*/jre/lib/`logging.properties`:

```
java -Djava.util.logging.config.file=/scratch/user/config/logging.properties
```

# L

# Rule and Fingerprint Logging

You can enable logging to help troubleshoot problems or test rules. In rule logging, rows are written to the VR_RULE_LOGS table.

In Oracle Adaptive Access Manager, rule logs are captured during the execution of various policies and rules at the different checkpoints (such as Pre-Authentication, Post-Authentication, and others).

Oracle Adaptive Access Manager supports two rule logging options:

- Detailed rule logging - Detailed rule logging captures the time taken at each rule level.

- Fingerprint rule logging - Fingerprint rule logging captures only the time taken at the policy level. Fingerprint rule logging reduces logging overhead in the database; thereby improving performance. In 11*g*, rule log fingerprinting is enabled by default.

Time taken values are performance statistics and the length of time that the rule or policy took to execute.

---

> **Note:** On a production machine, you want to manage the amount of time logging is enabled since increasing the amount of logging may negatively affect performance.

---

## L.1 About Rule Logging

Rule logging records the required rule processing information so that the Administrator can monitor the required information from a user session. Rule log details are captured in the VR_RULE_LOGS table while executing various policies and rules at different checkpoints.

### L.1.1 Fingerprint Rule Logging

Fingerprint rule logging records the policies and rules that were executed. Fingerprint-based logs are a shorter version of the rule logs; they do not include alert sources and per rule time, and so on. Fingerprint based logging is done to minimize data growth and also keep the logging overhead to a minimum. The fingerprint is a digest of a set of rules that were triggered. When a set of rules is triggered, a digest of the triggered rules is created and persisted in the database. The next time the same set of rules is triggered, the digest is reused and persisted so that the new session will have the same digest now for the runtime. When fingerprint logging is performed, the time required for the rule and policy execution is not captured and displays as -1 or N/A in the Session Details page. Fingerprint rule logging is enabled by default.

## L.1.2 Detailed Rule Logging

Detailed rule logging captures the captures the rules that were executed and the length of time that the rule or policy took to execute. The execution time is used as a performance statistic. Detailed rule logs are created only if the execution time is more than a threshold value that you have configure. On a production machine, you want to manage the amount of time before detailed logging is enabled since increasing the amount of logging may negatively affect performance. If the details are logged about the rules (runtime) that have a long execution time, the overhead for logging is decreased.

If the runtime requires an unusual amount of time, you might want to run detailed rule logging so that you can perform further analysis on why the rule took so long to run. Fingerprinting logging does not capture the timing information. Timing is an important factor in troubleshooting the "slow" runtime. In detailed logging, by default, only log timing for the rules that triggered are logged. The untriggered rules are not logged unless you specify you want to capture the untriggered rules also. Untriggered are captured in fingerprint rule logging.

## L.1.3 Status Columns in the VR_RULE_LOGS Table

The VR_RULE_LOGS table enables administrators to view the status of the rules. This information can be used for troubleshooting rules.

This status columns are explained in this section.

### 0 = notfired

The rule was tested but the conditions were not satisfied, so the rule was not triggered.

Rule logs are not always created for `notfired` status. There are properties that control whether the `notfired` status is shown or not.

If `vcrypt.tracker.rules.trace.notTriggered` is set to `false`, then rule logs for the `notfired` status are never created.

The property `vcrypt.tracker.rules.trace.notTriggered.logMillis` contains a threshold in milliseconds. If the rule executed in fewer milliseconds than this threshold, then the rule log will not be created.

If you want to always log `notfired` status rules, then set `vcrypt.tracker.rules.trace.notTriggered` to `true` and set `vcrypt.tracker.rules.trace.notTriggered.logMillis` to 0.

If you never want to log `notfired` status rules, then set `vcrypt.tracker.rules.trace.notTriggered` to false.

If you only want to log `notfired` status rules that take longer than a certain amount of time to test the conditions, then set `vcrypt.tracker.rules.trace.notTriggered` to `true` and set `vcrypt.tracker.rules.trace.notTriggered.logMillis` to the threshold millisecond value that you want.

### 1 = fired

The rule was tested and the conditions were satisfied, so the rule was triggered.

### 2 = override

This status is not used currently.

**3 = error**

An internal error occurred while testing this rule. Check the logs for more details.

**Status 4-8**

These columns all deals with preconditions. If the rule was not tested because preconditions were set up to exclude the device, city, state, country, or group, then the rule log will show a status that matches the precondition.

4 = deviceScoreExclude

5 = cityScoreExclude

6 = stateScoreExclude

7 = countryScoreExclude

8 = groupExclude

**99 = unknown**

You should never have a rule log with this status.

## L.2 Rule Logging Properties

Table L–1 shows the rule logging configuration properties.

*Table L–1    Rule Logging Properties*

| Properties | Description |
|---|---|
| vcrypt.tracker.rules.trace.policySet | True/False |
| | Enables rule logging. |
| vcrypt.tracker.rules.trace.policySet.*checkpoint* | True/False |
| | Enables rule logging. You can specify the checkpoint in which to log the rules. The variable *checkpoint* corresponds to the checkpoint. |
| | If the logging configuration is explicitly set at the given checkpoint, the Rules Engine uses that value; otherwise, it uses the value of vcrypt.tracker.rules.trace.policySet. |
| vcrypt.tracker.rules.trace.policySet.min.ms |  1000 (milliseconds) |
| | Specifies when to perform rule logging. You must configure this property to enable rule logging. You can configure this property for time so that logging is performed only if the total time taken for the runtime is greater than this value. The property, as set, logs for all runtime process rules only if the total time taken is more than 1000 ms. |
| | -1 |
| | If you are unable to see the rules log in the Session Details page with the above property value, change it to -1. |
| vcrypt.tracker.rules.trace.notTriggered | False |
| | If set to `true`, untriggered rules are logged along with the triggered rules |

*Table L–1   (Cont.)  Rule Logging Properties*

| Properties | Description |
|---|---|
| vcrypt.tracker.rules.trace.notTriggered.logMillis | Narrows down which rules are logged. |
|  | If the rule execution for untriggered rules exceeds the value specified then untriggered rules are logged. |
| vcrypt.tracker.rulelog.detailed.minMillis | 2000 |
|  | Determines the minimum time required for detailed logging. You can configure rule logging such that detailed rule logs are created only if the execution time is more than a threshold. That way, details are logged against the rules (runtime) with long execution time and hence the overhead of detailed logging is reduced. |
|  | Controls threshold for the logging for rules. By default, the Session Details page does not display the trigger sources if the execution time for alerts is less than 2000 millisecond (2000 ms) since detailed logging is dependent on the execution time. |
| vcrypt.tracker.rulelog.fingerprint.enabled | True/False |
|  | Enables fingerprint logging. |
| vcrypt.tracker.rulelog.exectime.maxlimit | Determine if fingerprint or detailed logging runs. If the value is exceeded, detailed logging is performed. Both are run if the property is set to -1. |

## L.3  Enabling Rule Logging

Enable rule logging by using the Properties editor. The steps are as follows:

1.  Log in to the OAAM Admin Console.

2.  In the Navigation pane, double-click **Properties** under the **Environment** node. The **Properties Search** page is displayed.

3.  Enter `vcrypt.tracker.rules.trace.policySet` in the **Name** field and click **Search**.

    You should see the property in the Search Results section.

4.  Click to select the property in the Search Results section.

5.  In the `vcrypt.tracker.rules.trace.policySet` details section, enter `true` in the **Value** field.

6.  Click **Save**.

    A confirmation dialog is displayed.

7.  Click **OK** to dismiss the dialog.

8.  If the property does not exists, from the Properties Search page, click the **New Property** button or **Create new Property** icon.

    A New Property dialog is displayed.

9.  In the New Property dialog, type in the property name and value.

10. Click **Create**.

## L.4  Enabling Rule Logging for a Specific Checkpoint

Enable rule logging for a specific checkpoint by using the Properties editor. The steps are as follows:

1.  Log in to the OAAM Admin Console.

2.  In the Navigation pane, double-click **Properties** under the **Environment** node. The **Properties Search** page is displayed.

3.  From the Properties Search page, click the **New Property** button or **Create new Property** icon.

    A New Property dialog is displayed.

4.  In the New Property dialog, type in `vcrypt.tracker.rules.trace.policySet.`*`checkpoint`* in the **Name** field.

5.  Enter `true` in the **Value** field and click **Create**.

To illustrate how rule logging for checkpoints is control by property combinations, a matrix is shown below. The Post-Authentication checkpoint is used to illustrate checkpoint rule logging flow.

The flow is as follows:

1.  The Rules Engine checks for a configuration for `vcrypt.tracker.rules.trace.policySet.postauth`.

2.  If there is no configuration for `vcrypt.tracker.rules.trace.policySet.postauth`, the Rules Engine checks the configuration value of `vcrypt.tracker.rules.trace.policySet`.

If the logging configuration is explicitly set at the given checkpoint, the Rules Engine uses that value; otherwise, it uses the value of `vcrypt.tracker.rules.trace.policySet`.

The following matrix shows an example of how value combinations control logging for a specified checkpoint.

| vcrypt.tracker.rules.trace.policySet.postauth | vcrypt.tracker.rules.trace.policySet | Checkpoint Rule logging enabled? |
| --- | --- | --- |
| true | false | yes |
| true | true | yes |
| true | not set | yes |
| false | false | no |
| false | true | no |
| false | not set | no |
| not set | false | no |
| not set | true | yes |
| not set | not set | yes |

## L.5  Enabling Logging of Untriggered Rules

To configure rule logging to log untriggered rules, use the Properties editor to set the following properties:

```
vcrypt.tracker.rules.trace.notTriggered=[true|false]
vcrypt.tracker.rules.trace.notTriggered.logMillis=[millis]
```

The value of `vcrypt.tracker.rules.trace.notTriggered` adds rules to log. If set to `true`, rules that are not triggered are logged along with the triggered rules.

The value of `vcrypt.tracker.rules.trace.notTriggered.logMillis` narrows down which rules are logged.

If the rule execution for untriggered rules exceeds the value of `vcrypt.tracker.rules.trace.notTriggered.logMillis`, only then will the Rules Engine log the untriggered Rules.

The following table shows the property values that control rule logging for untriggered rules.

| vcrypt.tracker.rules.trace.notTriggered | vcrypt.tracker.rules.trace.notTriggered.logMillis | Result |
| --- | --- | --- |
| true | n | Logs the untriggered Rules that took more than "n" milliseconds. If "n" is set to a negative value, all rules are logged |
| false | n | None of the untriggered rules are logged |

## L.6 Enabling Detailed Logging

Configure the minimum time required for detailed logging so that details are logged for rules (runtimes) that have long execution times. Detailed rule logs are created only if the execution time is more than a threshold.

1. In the Navigation tree, double-click **Properties** under **Environment**.

2. Enter **vcrypt.tracker.rulelog.detailed.minMillis** in the **Name** field and click **Search**.

3. In the Results table, select **vcrypt.tracker.rulelog.detailed.minMillis**.

4. In the Details vcrypt.tracker.rulelog.detailed.minMillis section, edit the value in the **Value** field.

5. Click **Save**.

   A confirmation dialog is displayed.

6. Click **OK** to dismiss the dialog.

If a policy takes more than "n" in milliseconds specified, Oracle Adaptive Access Manager starts the detailed rule logging.

## L.7 Enabling Fingerprint Rule Logging

To enable or disable fingerprint rule logging, modify the following property using the Property editor:

```
vcrypt.tracker.rulelog.fingerprint.enabled=true
```

## L.8 Other Fingerprint and Detailed Logging Properties

Properties can be set for

- Running either fingerprint or detailed logging

- Running both fingerprint and detailed logging and when

- Fingerprint logging threshold

### Specify Whether Fingerprint or Detailed Logging Runs

To set a property to determine if fingerprint or detailed logging runs, set

```
vcrypt.tracker.rulelog.exectime.maxlimit
```

If the value is exceeded, detailed logging is performed.

### Specify to Include Other Limits

To include all specified properties in determining the use of both, set

```
vcrypt.tracker.rulelog.exectime.maxlimit=-1
```

### Specify Not to Use Both

To specify to perform logging with both logging mechanisms (detailed and fingerprint), set

```
vcrypt.tracker.rulelog.logBoth
```

to true. The value overrides `vcrypt.tracker.rulelog.exectime.maxlimit`.

### Configuring Fingerprint Logging Threshold Time

To modify the threshold time after which fingerprint rule logging should be used, set the following property in milliseconds:

```
vcrypt.tracker.rulelog.exectime.maxlimit=
```

## L.9 Archiving and Purging Rule Log Data

The OAAM archive and purge script will archive and purge all rule log data that is 30 days old, but you should set the value based on the customer care requirement. If the reporting database is used, then, rule logging data retention should be less than 30 days.

*Table L–2    Rules and Policy Log Data Tables*

| Rules, Policy Log Tables | Corresponding Archived Tables |
|---|---|
| VR_POLICYSET_LOGS | VR_POLICYSET_LOGS_PURGE |
| VR_RULE_LOGS | VR_RULE_LOGS_PURGE |
| VR_MODEL_LOGS | VR_MODEL_LOGS_PURGE |
| VR_POLICY_LOGS | VR_POLICY_LOGS_PURGE |

# Glossary

**Abbreviation**

This algorithm handles common abbreviations, common nicknames, common acronyms, and date format.

**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**

Rule result which can impact users such forcing them to register a security profile, KBA-challenging them, blocking access, asking them for PIN or password, and so on.

**Actions Group**

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.

**Adaptive Risk Manager**

A category of Oracle Adaptive Access Manager features. Business and risk analytics, fraud investigation and customer service tools fall under the Adaptive Risk Manager category.

**Adaptive Strong Authenticator**

A category of Oracle Adaptive Access Manager features. All the end-user facing interfaces, flows, and authentication methods fall under the Adaptive Strong Authenticator category.

**Alert**

Rule results containing messages targeted to specific types of Oracle Adaptive Access Manager users.

**Alert Group**

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.

### Answer Logic

Answer Logic is a unique combination of Knowledge Based Authentication with registration, answer, and fuzzy logic to enable KBA for the Identity and Access Management Suite.

### Attribute

Attributes are the particular pieces of information associated with the activity being tracked. An example is the time of day for a login. Patterns collect data about members. If the member type is **User**, the pattern will collect data about users.

### 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?"

### Authentication Status

Authentication Status is the status of the session (each login/transaction attempt creates a new session).

Examples are listed below:

- If a user logs in for the first time and he goes through the registration process, but decides not to complete the registration process and logs out, the authentication status for this user session is set as "Pending Activation."

- If a user logs in from a different device/location, he is challenged. He answers the challenge questions incorrectly in all the three attempts, the authentication status for this session is set as "Wrong Password."

- If a user logs in and is taken to the final transaction page or success page, the authentication status for the particular session is set as "Success."

- If the user is a fraud and is blocked, the status for the session is set as "Block."

### Authorization

Authorization regards the question "Who can access what resources offered by which components?"

### Autolearning

Autolearning is a set of features in Oracle Adaptive Access Manager that dynamically profile behavior in real-time. The behavior of users, devices and locations are recorded and used to evaluate the risk of current behavior.

### Black List

A given list of users, devices, IP addresses, networks, countries, and so on that are blocked. An attack from a given member can show up on a report and be manually added to a blacklist at the administrator's discretion.

### Blocked

If a user is "Blocked," it is because a policy 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.

**Browser Fingerprinting**

When the user accesses the system, OAAM collects information about the computer. By combining all that data, the site creates a fingerprint of the user's browser. This fingerprint could potentially uniquely identify the user. Information gathered that makes up the browser fingerprint include the browser type used, plug-ins installed, system fonts, and the configuration and version information from the operating system, and whether or not the computer accepts cookies.

The browser and flash fingerprints are tracked separately. The fingerprints are available in the session listing and details pages and you can get further details about the fingerprint by opening the respective details pages. Hence, you can have both fingerprints available, but if the user has not installed flash then the digital fingerprint (flash) is set to null.

**Buckets**

Patterns are configured by an administrator and Oracle Adaptive Access Manager uses that configuration to create buckets as it needs them. Administrators do not deal or see buckets directly in any way.

Patterns are configured to create either one bucket or multiple buckets. Buckets are containers that are used to capture the frequency of behaviors. Rules evaluate the counters in these buckets for specific members to determine if a situation is anomalous.

**Cache Data**

Information about historical data during a specified time frame

**Cache Policy**

Groups offer two Cache 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 and read-only groups are good candidates for the "Full Cache" option. Administrators must 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" Cache Policy option does not use cache and consults the database every time. Device group types are set to "None" because in most cases, they are dynamic and manipulated while the server is running. If you have groups that stay static for the lifetime of the server, you can use the "Full Cache" option instead of "None."

**Case**

**Cases** provide tools to track and solve customer service issues.

A **case** is a record of all the actions performed by the CSR to assist the customer as well as various account activities of the customer. Each case is allocated a **case number**, a unique case identification number.

**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. The customer support representatives can use the CSR set of tools for handling inquiries associated with Oracle Adaptive Access Manager. A CSR case is attached to a user.

- Escalated - When a CSR Manager identifies that a particular case needs additional investigation and escalates the case and the CSR Case becomes an escalated case. It is associated with a user.

**Challenge Questions**

Challenge Questions are a finite list of questions used for secondary authentication.

During registration, users are presented with several question menus. For example, he may be presented with three question menus. A user must select one question from each menu and enter answers for them during registration. Only one question from each question menu can be registered. These questions become the user's "registered questions."

When rules in OAAM Admin trigger challenge questions, OAAM Server displays the challenge questions and accepts the answers in a secure way for users. The questions can be presented in the QuestionPad, TextPad, and other pads, where the challenge question is embedded into the image of the authenticator, or simple HTML.

**Challenge Type**

Configuration of a type of challenge (ChallengeEmail, ChallengeSMS, ChallengeQuestion)

**Checkpoint**

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

Examples of checkpoints are:

- Pre-authentication - Rules are run before a user completes the authentication process.

- Post-authentication - Rules are run after a user is successfully authenticated.

**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 challenge questions/answers and email/cell phone.

**Condition**

Conditions are configurable evaluation statements used in the evaluation of historical and runtime data.

**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)**

Patterns are configured to create either one bucket or multiple buckets. Buckets are containers that are used to capture the frequency of behaviors. Rules evaluate the counters in these buckets for specific members to determine if a situation is anomalous.

- Single-bucket patterns 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 is created and populated with users. If a user logs in from the United States, he or she becomes a member of the bucket and the bucket counts are incremented; if he or she does not log in from the United States, the bucket count is not incremented.

- Multi-bucket patterns usually create more buckets than single-bucket patterns. They create buckets as required based on the parameter configurations.

  You configure the data types and samples you want Oracle Adaptive Access Manager to generate buckets from, and then during pattern processing Oracle Adaptive Access Manager creates buckets as needed to capture behaviors.

**CSR**

Customer service representatives resolve low risk customer issues originating from customer calls. CSRs has limited access to OAAM Admin

- 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 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.

### Dashboard

Provides a real-time view of activity via aggregates and trending.

### Data Elements

An entity is a set of attributes. Data elements are what is used to describe the attributes that make up an entity. For example, the credit card entity has attributes such as address line 1, address line 2, city, zip, and state. Data elements, such as description, length, type, and so on, are used to describe each attribute.

### Data Mining

Data mining is the practice of automatically searching large stores of data to discover patterns and trends that go beyond simple analysis. Data mining uses sophisticated mathematical algorithms to segment the data and evaluate the probability of future events. Data mining is also known as Knowledge Discovery in Data (KDD). Data mining can answer questions that cannot be addressed through simple query and reporting techniques.

### Data Type

An attribute of data that represents the kind and structure of the data. For example, String.

### 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

### Delivery Channel

Delivery mechanism used to send the OTP to the user. Email, SMS, IM, and so on are delivery channels.

### Device

A computer, PDA, cell phone, kiosk, etc used by a user

### Device Fingerprinting

Device fingerprinting collects information about the device such as browser type, browser headers, operating system type, locale, and so on. Fingerprint data represents the data collected for a device during the login process that is required to identify the device whenever it is used to log in. 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. The fingerprint details help in identifying a device, check whether it is secure, and determine the risk level for the authentication or transaction.

A customer typically uses these devices to log in: desktop computer, laptop computer, PDA, cell phone, kiosk, or other web enabled device.

### Device Identification

During the registration process, the user is given an option to register his device to the system. If a user tries to login from a registered device, the application knows that it is

a safe and secure device and allows the user to proceed with his transactions. This process is also called device identification.

### Digest Identification Scheme

The Digest Identification Scheme creates a unique identifier by hashing the values of the selected elements of the entity. The resultant key is usually cryptic.

### display scheme

The display scheme consists of the elements you want to present and the order when you want to display the value of an entity in a user interface. For example, if you want to display an address, you would want to show address line 1 as the first item, address line 2 as the second item, city as the third item, state as the fourth item, and zipcode as the fifth item.

### Disposition

The disposition describes the way in which the issue was resolved in a case. Cases only have dispositions when they are 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) being used as a safe device. The customer can then configure the rules to challenge a user that is not coming from one of the registered devices.

Once the feature is enabled, information about the device is collected for that user. To make use of the information being collected, policies must be created and configured. For example, a policy could be created with rules to challenge a user who is not logging in from one of the registered devices.

### encrypted

Information that is made unreadable to anyone except those possessing special knowledge

### Entities Editor

A tool to edit entities, a user-defined structure that can be reused across different transactions. Only appropriate and related fields should be grouped into an Entity.

### Entity

An entity is a user-defined data structure that can be re-used across different transactions.

### Environment

Tools for the configuration system properties and snapshots

### 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 changes from the current status to Expired. The case could be in pending, escalated statuses when it expires. After the case expires, the user will not be able to open the case anymore, but the CSR Manager can. The length of time before a case expires is configurable.

### Execution Types

Two execution types for configurable actions are listed:

- Synchronous - Synchronous actions are executed in the order of their priority in ascending order. For example, if the user wants to create a case and then send an email with the Case ID, the user would choose synchronous actions. Synchronous actions will trigger/execute immediately.

  If the actions are executing in sequential order and one of the actions in the sequence does not trigger, the other actions will still trigger.

- Asynchronous actions are queued for execution but not in any particular sequence. For example, if you want to send an email or perform some action and do not care about executing it immediately and are not interested in any order of execution, you would choose asynchronous actions.

### Enumerations

User-defined enums are a collection of properties that represent a list of items. Each element in the list may contain several different attributes. The definition of a user-defined enum begins with a property ending in the keyword ".enum" and has a value describing the use of the user-defined enum. Each element definition then starts with the same property name as the enum, and adds on an element name and has a value of a unique integer as an ID. The attributes of the element follow the same pattern, beginning with the property name of the element, followed by the attribute name, with the appropriate value for that attribute.

The following is an example of an enum defining credentials displayed on the login screen of an OAAM Server implementation:

```
bharosa.uio.default.credentials.enum = Enum for Login Credentials
bharosa.uio.default.credentials.enum.companyid=0
bharosa.uio.default.credentials.enum.companyid.name=CompanyID
bharosa.uio.default.credentials.enum.companyid.description=Company ID
bharosa.uio.default.credentials.enum.companyid.inputname=comapanyid
bharosa.uio.default.credentials.enum.companyid.maxlength=24
bharosa.uio.default.credentials.enum.companyid.order=0
bharosa.uio.default.credentials.enum.username=1
bharosa.uio.default.credentials.enum.username.name=Username
bharosa.uio.default.credentials.enum.username.description=Username
bharosa.uio.default.credentials.enum.username.inputname=userid
bharosa.uio.default.credentials.enum.username.maxlength=18
bharosa.uio.default.credentials.enum.username.order=1
```

### Evaluation Priority

The priority in which the collected data is evaluated:

- High

  Most of the resources are assigned for the data to be evaluated.

- Low

  The resources assigned to data evaluation is half as much as the High priority.

### Fat Fingering

This algorithm handles Answers with typos due to the proximity of keys on a standard keyboard.

### Flash Fingerprinting

Flash fingerprinting is similar to browser fingerprinting but a flash movie is used by the server to set or retrieve a cookie from the user's machine so a specific set of

information is collected from the browser and from flash. The flash fingerprint is only information if flash is installed on the client machine.

The fingerprints are tracked separately. The fingerprints are available in the session listing and details pages and you can get further details about the fingerprint by opening the respective details pages. Hence, you can have both fingerprints available, but if the user has not installed flash then the digital fingerprint (flash) is set to null.

### Fraud Investigator

A Fraud Investigator primarily looks into suspicious situations either escalated from customer service or directly from Oracle Adaptive Access 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. An Investigation Manager must routinely search for expired cases to make sure none are pending.

### Fraud Scenario

A fraud scenario is a potential or actual deceptive situation involving malicious activity directed at a company's online application.

For example, you have just arrived at the office on Monday and logged into OAAM Admin. You notice that there are a high number of logins with the status "Wrong Password" and "Invalid User" coming in from a few users. Some appear to be coming in from different countries, and some appear to be local. You receive a call from the fraud team notifying you that some accounts have been compromised. You must come up with a set of rules that can identify and block these transactions.

### Gated Security

The multiple security checkpoints a user must pass through to gain access to sensitive data or transactions.

### Grey List

Anyone not in the black list and white list. Grey list members are subject to various levels of challenges.

### Groups

Collection of like items. Groups are found in the following situations

- Groups are used in rule conditions

- Groups that link policy to user groups

- Action and alert groups

### HTTP

Hypertext Transfer Protocol

### ID Scheme

An ID scheme consists of the data elements that can uniquely identify an entity, in other words, you are defining the unique combination that identifies the entity. For example, the credit card entity has many attributes, but the way to uniquely identify a credit card is by using the 16-digit credit card number. In that case, the ID scheme is just the credit card number.

Another example, the address entity has address line 1, address line 2, city, state, and zipcode as attributes. Address line 1, address line 2, and zipcode, without the state and city attributes, can still be used to identify the address uniquely.

**IP address**

Internet Protocol (IP) address

**Job**

A job is a collection of tasks that can be run by OAAM. You can perform a variety of jobs such as load data, run risk evaluation, roll up monitor data, and other jobs.

**KBA Phone Challenge**

Users can be authenticated over the phone using their registered challenge questions. This option is not available for unregistered users or in deployments not using KBA.

**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.

**Key Identification Scheme**

The Key Identification Scheme creates a unique identifier by simply concatenating the selected elements of the entity.

**Knowledge Based Authentication (KBA)**

OAAM knowledge based authentication (KBA) is a user challenge infrastructure based on registered challenge questions. It handles Registration Logic, challenge logic, and Answer Logic.

**Last Case Action**

The last action executed in the CSR case.

**Last Global Case Action**

The last action that occurred for this user in all CSR cases. 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 KBA or OTP challenge. The "Locked" status is only used if the KBA or One Time-Password (OTP) facility is in use.

- OTP: OTP sends a one-time PIN or password to the user through a configured delivery method, and if the user exceeds the number of retries when attempting to provide the OTP code, the account becomes "Locked."

- KBA: For online challenges, a customer is locked out of the session when the Online Counter reaches the maximum number of failures. For phone challenges, a customer is locked out when the maximum number of failures is reached and no challenge questions are left.

After the lock out, 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

### Member

Member represents the actor in the system.

### Multifactor Authentication

Multifactor authentication (MFA) is a security system in which more than one form of authentication is implemented to verify the legitimacy of a transaction. In contrast, single factor authentication (SFA) involves only a User ID and password.

### Multiprocessing Modules (MPMs)

Apache httpd ships with a selection of Multi-Processing Modules (MPMs) which are responsible for binding to network ports on the machine, accepting requests, and dispatching children to handle the requests.

### 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 Policies

A nested policy is a secondary policy used to further quantify the risk score in instances where the original result output by the system is inconclusive. Nested Policies can be assigned to ensure a higher degree of accuracy for the risk score. A nested policy is run only when a specific sequence of answers is returned from the primary policy. Nested policies therefore reduce false positives and negatives.

### OAAM Admin

Administration Web application for all environment and Adaptive Risk Manager and Adaptive Strong Authenticator features.

### OAAM Server

Adaptive Risk Manager and Adaptive Strong Authenticator features, Web services, LDAP integration and user Web application used in all deployment types except native integration

### One Time Password (OTP)

One Time Password (OTP) is a form of out of band authentication that is used as a secondary credential and generated at pre-configured checkpoints based on the policies configured.

### OTP Anywhere

OTP Anywhere is a risk-based challenge solution consisting of a server generated one time password delivered to an end user via a configured out of band channel. Supported OTP delivery channels include short message service (SMS), eMail, instant messaging and voice. OTP Anywhere can be used to compliment KBA challenge or instead of KBA. As well both OTP Anywhere and KBA can be used alongside practically any other authentication type required in a deployment. Oracle Adaptive Access Manager also provides a challenge processor framework. This framework can be used to implement custom risk-based challenge solutions combining third party authentication products or services with OAAM real-time risk evaluations.

### Oracle Adaptive Access Manager

A product to protect the enterprise and its customers online.

Oracle Adaptive Access Manager

- provides multifactor authentication security

- evaluates multiple data types to determine risk in real-time

- aids in research and development of fraud policies in offline environment

- integrates with access management applications

Oracle Adaptive Access Manager is composed of two primary components: OAAM Server and OAAM Admin.

### Oracle Data Mining (ODM)

Oracle Data Mining is an option to the Oracle Database EE, provides powerful data mining functionality

### Order

The order determines how the data is concatenated while forming the data that identifies the entity.

### Organization ID

The unique ID for the organization the user belongs in

### Out Of Band Authentication

The use of two separate networks working simultaneously to authenticate a user. For example: email, SMS, phone, and so on.

### Pattern

Patterns are configured by an administrator and record the behavior of the users, device and locations accessing the system by creating a digest of the access data. The digest or profile information is then stored in a historical data table. Rules evaluate the patterns to dynamically assess risk levels.

### Pattern Name

Patterns are features characteristic of an individual or a group. Usually these patterns represent behavior considered to be high risk based on industry expertise.

**Pattern Status**

Status is the current state of a Pattern. There are 4 states in pattern creation.

- Active

  If data must be collected, the pattern must be in the active state.

- Inactive

  If the pattern is complete, but you do not want to collect data, select **Inactive**.

- Incomplete

  If pattern creation has started, but you need to save it for completion later, select **Incomplete**. Data is not collected for this state.

- Invalid

  The administrator may choose to mark the pattern as invalid if he or she does not want the pattern used. Data is not collected for this state.

**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 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 user names, 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.

**Phonetics**

This algorithm handles Answers that "sound like" the registered answer, regional spelling differences, and common misspellings

**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**

Policies contain security rules and configurations used to evaluate the level of risk at each checkpoint.

**Policy Set**

A policy set is the collection of all the currently configured policies used to evaluate traffic to identify possible risks. The policy set contains the scoring engine and action/score overrides.

**Policy Status**

Policy has three status which defines the state of the object or its availability for business processes.

- Active
- Disabled
- Deleted

Deleted is not used.

When a policy is deleted, it is permanently deleted from the database.

By Default every new policy created has status as "Active."

Every copied policy has a default status as "Disabled."

**Predictive Analysis**

Predictive analytics encompasses a variety of techniques from statistics, data mining and game theory that analyze current and historical facts to make predictions about future events.

**Questions Active**

Status of the user who has completed registration and questions exists by which he can be challenged.

**Question Set**

The total number of questions a customer can choose from when registering challenge questions.

**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.

**Registered Questions**

A customer's registered questions are the questions that he selected and answered during registration or reset. Only one question from each question menu can be registered.

**Registration Logic**

The configuration of logic that governs the KBA registration process.

**Risk Score**

The numeric risk level associated with a checkpoint.

**Row and Column**

In element definition, row and column is the location where data is stored in the database. The row and column are automatically assigned. It is optional for the administrator to change these.

**Rule Conditions**

Conditions are the basic building blocks for security policies.

**Rules**

Rules are a collection of conditions used to evaluate user activity.

### Scores

Score refers to the numeric scoring used to evaluate the risk level associated with a specific situation. A policy results in a score.

### Scoring Engine

Oracle Adaptive Access Manager uses scoring engines to calculate the risk associated with access requests, events, and transaction.

Scoring engines are used at the policy and policy set levels. The Policy Scoring Engine is used to calculate the score produced by the different rules in a policy. The Policy Set Scoring Engine is used to calculate the final score based on the scores of policies.

Where there are numerous inputs, scoring is a able to summarize all these various points into a score that decisions can be based on.

### 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." For example, if the customer wants a different image, then the severity level assigned is "Low." Severity levels of a case can be escalated or deescalated 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

### Snapshot

A snapshot is a zip file that contains Oracle Adaptive Access policies, dependent components and configurations for backup, disaster recovery and migration. Snapshots can be saved to the database for fast recovery or to a file for migration between environments and backup. Restoring a snapshot is a process that includes visibility into exactly what the delta is and what actions will be taken to resolve conflicts. For information on snapshots, refer to Chapter 16, "Managing System Snapshots."

### 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.

**Source Data**

All parameters (data fields) for the transaction from the external application (client's end) that will be sent to the Oracle Adaptive Access Manager Server.

**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.

**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. TextPad is often deployed as the default for all users in a large deployment then each user individually can upgrade to another device if they wish. The personal image and phrase a user registers and sees every time they login to the valid site serves as a shared secret between user and server.

**Transaction**

A transaction defines the data structure and mapping to support application event/transaction analytics.

**Transaction Data**

Data that is an abstract item or that does not have any attributes by itself, does not fit into any entity, which exists or is unique by itself is defined as transaction data.

Items that cannot fall into an entity are classified as standalone data.

A classic example is amount or code.

**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.

**Transaction Key**

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

**Trigger**

A rule evaluating to true.

**Transaction Type**

The Transaction Definitions that have been configured in this specific installation such as authentication, bill pay, wire transfer, and others.

**Trigger Combinations**

Additional results and/or policy evaluation based on rule outcome combinations. You can specify a score, action group and alert group based on different rule outcome combinations or you can point to a nested policies to further evaluate the risk.

**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.

**Validations**

Answer validation used in the KBA question registration and challenge process

**Virtual Authentication Devices**

A personalized device for entering a password or PIN or an authentication credential entry device. The virtual authentication devices harden the process of entering and transmitting authentication credentials and provide end users with verification they are authenticating on the valid application.

**Virus**

A computer program that can copy itself and infect multiple computers without permission or knowledge of the users.

**White List**

A list of trusted members. Any activity that originates from these users, devices, IP addresses, networks, countries, and so on can be trusted.

# Index