

Oracle® Fusion Middleware

Administrator's Guide for Oracle Adaptive Access Manager

Release 11g (11.1.1)

E14568-02

August 2010

Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager, Release 11g (11.1.1)
E14568-02

Copyright © 2009, 2010, Oracle and/or its affiliates. All rights reserved.

Primary Author: Priscilla Lee

Contributors: Mandar Bhatkhande, Roopang Chauhan, Sree Chitturi, Josh Davis, Jordan Douglas, Bosco Durai, Philomina Dorai, Arunkumar Jayaraman, Daniel Joyce, Mark Karlstrand, Wei Jie Lee, Derick Leo, Srinivas Nagandla, Madhan Neethiraj, Paresh Raote, Uday Sambhara, Kamal Singh, Nandini Subramani, Elangovan Subramanian, Vidhya Subramanian, Dawn Tyler, and Sachchidanand Vanungare

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	xxvii
Audience	xxvii
Documentation Accessibility	xxviii
Related Documents	xxviii
Conventions	xxix
What's New in Oracle Adaptive Access Manager 11g Release 1 (11.1.1)?	xxxi
New Features for Oracle Adaptive Access Manager 11g Release 1 (11.1.1)	xxxi
Feature Comparison Chart - Oracle Adaptive Access Manager 11g vs. Oracle Adaptive Access Manager 10g	xxxii
Concepts and Terminology Changes for Oracle Adaptive Access Manager 11g	xxxiv
Part I Getting Started with Oracle Adaptive Access Manager	
1 Introduction to Oracle Adaptive Access Manager	
1.1 Benefits of Oracle Adaptive Access Manager	1-2
1.2 Oracle Adaptive Access Manager Features	1-2
1.3 Oracle Adaptive Access Manager User Roles	1-4
1.4 Oracle Adaptive Access Manager Integrations	1-4
1.4.1 Native Integration	1-4
1.4.2 Reverse Proxy Integration	1-5
1.4.3 Access Management Integration	1-5
1.4.4 SAML Integration	1-5
1.5 Oracle Adaptive Access Manager Architecture	1-5
1.5.1 Architectural Scenario for Deployment	1-5
2 Setting Up the Oracle Adaptive Access Manager Environment	
2.1 Installation and Configuration	2-1
2.2 Setting Up the Oracle Adaptive Access Manager Basic Environment	2-1
2.3 Setting Up CLI Environment	2-2
2.4 Setting Up Encryption and Database Credentials for Oracle Adaptive Access Manager	2-2
2.4.1 Overview of the Process	2-2
2.4.1.1 Setting up Encryption	2-2
2.4.1.2 Configuring Database Credentials in the Credential Store Framework	2-2
2.4.2 Pre-requisites	2-3

2.4.3	Setting up Secret Key for Encrypting Configuration Values	2-3
2.4.4	Setting Up Secret Key for Encrypting Database Values.....	2-4
2.4.5	Generating an Encoded Secret Key.....	2-5
2.4.6	Adding Symmetric Key to the Credential Store Framework.....	2-5
2.4.7	Setting Up Oracle Adaptive Access Manager Database Credentials in the Credential Store Framework 2-6	
2.4.8	Backing Up Secret Keys	2-6
2.5	Importing Challenge Questions.....	2-6
2.6	Importing Base Policies.....	2-7
2.7	Importing Conditions Library.....	2-8
2.8	Importing Configurable Action Templates.....	2-8
2.9	Importing Basic Authentication-Related Entities.....	2-8
2.10	Importing IP Location Data	2-8
2.11	Setting Properties to Enable Autolearning and Configurable Actions	2-9
2.12	Setting the Time Zone Used for All Time Stamps in OAAM Admin	2-9
2.12.1	Values for the Common Timezones.....	2-9

3 Oracle Adaptive Access Manager Navigation

3.1	Access Level to OAAM Admin.....	3-1
3.2	Signing In to Oracle Adaptive Access Manager 11g.....	3-2
3.3	OAAM Admin Console and Controls	3-3
3.4	Navigation Panel.....	3-4
3.5	Navigation Tree.....	3-5
3.5.1	Navigation Tree Structure	3-5
3.5.2	Navigation Tree Menu and Toolbar	3-6
3.6	Policy Tree.....	3-9
3.7	Management Pages.....	3-11
3.7.1	Search Pages	3-12
3.7.1.1	Elements in the Search Form.....	3-13
3.7.1.2	Search Results Table.....	3-13
3.7.1.3	Search Results Menu and Toolbar.....	3-14
3.7.1.4	Select All	3-15
3.7.1.5	Create and Import	3-15
3.7.2	Detail Pages	3-16
3.8	Dashboard.....	3-16
3.9	Access to Search, Create, and Import.....	3-16
3.10	Online Help.....	3-17

Part II Customer Service and Forensics

4 Managing and Supporting Cases

4.1	Introduction and Concepts.....	4-2
4.1.1	Case.....	4-2
4.1.1.1	CSR Cases	4-2
4.1.1.2	Escalated Cases	4-2
4.1.2	Customer Service Representative (CSR)	4-2
4.1.3	CSR Manager.....	4-3

4.1.4	Fraud Investigator	4-3
4.1.5	Fraud Investigation Manager.....	4-3
4.1.6	Locked Status	4-3
4.1.7	Temporary Allow	4-3
4.1.8	Case Status.....	4-4
4.1.9	Severity Level.....	4-4
4.1.10	Expiration Date	4-4
4.1.11	Customer Resets.....	4-4
4.2	CSR and CSR Manager Role Permissions	4-5
4.3	Getting Started.....	4-5
4.4	Cases Search Page	4-6
4.4.1	Searching for Cases.....	4-6
4.4.2	Viewing a List of Cases	4-8
4.4.3	Searching for Open and Closed Cases.....	4-8
4.4.4	Searching Case by Description Keyword.....	4-9
4.4.5	Viewing a List of Cases	4-9
4.5	Case Details Page	4-9
4.5.1	Case Actions	4-10
4.5.2	Viewing Case Details	4-10
4.5.3	Viewing User Details.....	4-10
4.6	Viewing Case Activity.....	4-11
4.6.1	Viewing the Case History	4-11
4.6.2	Searching the Log of a Case	4-12
4.6.3	Viewing Escalated Case Logs and Notes	4-12
4.7	Viewing Customer's Sessions.....	4-12
4.7.1	Viewing a Customer's Session History.....	4-13
4.7.2	Searching for a Customer's Sessions	4-13
4.7.3	Searching for a Customer's Sessions by Device ID or Date Range.....	4-13
4.7.4	Filtering the Session History by Authentication Status or Alert Level.....	4-14
4.7.5	Viewing Transactions in the Sessions History	4-14
4.8	Creating a CSR Case	4-14
4.8.1	Creating a Case	4-14
4.8.2	Creating a Case Like Another Case.....	4-16
4.9	Bulk-Editing CSR Cases (CSR Manager Only)	4-17
4.10	Performing Customer Resets.....	4-18
4.10.1	Resetting Image.....	4-18
4.10.2	Resetting Phrase.....	4-19
4.10.3	Resetting Image and Phrase	4-20
4.10.4	Unregistering Devices.....	4-20
4.10.5	Resetting OTP Profile	4-20
4.10.6	Resetting Virtual Authentication Device	4-21
4.10.7	Unlock OTP	4-21
4.10.8	Resetting a Customer's Challenge Questions, Question Set, Image, and Phrase....	4-22
4.11	Performing Challenge Question Resets.....	4-22
4.11.1	Performing Challenge Questions Related Actions	4-22
4.11.2	Resetting Challenge Questions	4-23
4.11.3	Resetting Challenge Questions and the Question Set	4-23

4.11.4	Incrementing a Customer to His Next Question.....	4-24
4.11.5	Unlocking a Customer (KBA)	4-24
4.11.6	Performing KBA Phone Challenge	4-24
4.12	Enabling a Temporary Allow (CSR Manager Only).....	4-25
4.13	Adding Notes to Cases.....	4-25
4.14	Changing Severity Level of a Case	4-26
4.15	Changing Status of a Case	4-26
4.15.1	Changing Case Status to Pending	4-27
4.15.2	Closing a Case	4-28
4.15.3	Reopening Closed Cases (CSR Manager Only).....	4-28
4.16	Extending Expiration (CSR Manager Only).....	4-29
4.17	Escalating Cases	4-29
4.18	Configuring Expiry Behavior for CSR Cases	4-29
4.19	Reporting.....	4-30
4.20	Use Cases.....	4-30
4.20.1	Use Case: Customer Session Search and Case Creation	4-30
4.20.2	Use Case: Reset Challenge Questions	4-30
4.20.3	Use Case: Reset Image and Phrase	4-32
4.20.4	Use Case: Bulk Edit CSR Cases.....	4-33
4.20.5	Use Case: CSR Manager Bulk Case Edit.....	4-34
4.21	Best Practices and Recommendations.....	4-35

5 Using Session Details

5.1	Getting Started.....	5-1
5.2	Searching for a Session.....	5-1
5.3	Navigating to the Session Details Page	5-2
5.4	Viewing Session Details	5-3
5.4.1	The Panels	5-3
5.4.2	Session Details Panel.....	5-3
5.4.3	Login Details Panel.....	5-3
5.4.4	Checkpoint Panels	5-3
5.4.5	Transactions Panel.....	5-4
5.4.6	Policy Explorer	5-4
5.5	Uses Cases	5-4
5.5.1	Use Case: Search Sessions.....	5-5
5.5.2	Use Case: Session Details Page	5-5
5.6	Comparison Between 10g and 11g Session Details	5-6

Part III Managing KBA and OTP

6 Managing Knowledge-Based Authentication

6.1	Introduction and Concepts.....	6-1
6.1.1	Knowledge Based Authentication.....	6-1
6.1.2	Challenge Response Process	6-2
6.1.3	Challenge Response Configuration.....	6-2
6.1.4	Registration.....	6-2

6.1.5	Challenge Questions.....	6-3
6.1.6	Question Set.....	6-3
6.1.7	Registration Logic.....	6-3
6.1.8	Answer Logic.....	6-5
6.1.9	Validations.....	6-6
6.1.10	Failure Counters.....	6-7
6.1.11	KBA Resets.....	6-7
6.1.11.1	Reset Challenge Questions.....	6-7
6.1.11.2	Reset Challenge Questions and the Set of Questions to Choose From.....	6-7
6.1.11.3	Increment User to the Next Question.....	6-8
6.1.11.4	Unlock a User.....	6-8
6.1.11.5	Ask Question (KBA Phone Challenge).....	6-8
6.1.12	Disable Question and Category Logic.....	6-8
6.1.13	Locked Status.....	6-9
6.2	Setting Up KBA Overview.....	6-9
6.2.1	Loading Challenge Questions.....	6-9
6.2.2	Setting Up KBA.....	6-9
6.2.3	Setting Up Challenge.....	6-10
6.2.4	User Flow.....	6-10
6.3	Setting Up the System to Use Challenge Questions.....	6-12
6.3.1	Ensuring that Universal Installation Option Base Policies are Installed.....	6-12
6.3.2	Ensuring that KBA Properties/Default Properties are Set.....	6-12
6.3.3	Uploading Challenge Questions.....	6-12
6.3.4	Importing and Enabling Policies.....	6-13
6.3.5	Configuring Rules for Registration and Challenge Policies.....	6-13
6.4	Accessing Configurations in KBA Administration.....	6-13
6.5	Managing Challenge Questions.....	6-13
6.5.1	Searching for a Challenge Question.....	6-14
6.5.2	Viewing Question Details and Statistics.....	6-16
6.5.3	Creating a New Question.....	6-16
6.5.4	Creating a Question Like Another Question.....	6-17
6.5.5	Editing a Question.....	6-18
6.5.6	Importing Questions.....	6-18
6.5.7	Exporting Questions.....	6-18
6.5.8	Deleting a Question.....	6-19
6.5.9	Disabling a Question.....	6-19
6.5.10	Activating Questions.....	6-20
6.5.11	Deactivating Questions.....	6-20
6.6	Setting Up Validations for Answer Registration.....	6-20
6.6.1	Using the Validations Page.....	6-20
6.6.2	Adding a New Validation.....	6-21
6.6.3	Editing an Existing Validation.....	6-23
6.6.4	Exporting Validations.....	6-23
6.6.5	Deleting Validations.....	6-24
6.7	Managing Categories.....	6-24
6.7.1	Searching for a Category.....	6-24
6.7.2	Creating a New Category.....	6-25

6.7.3	Editing a Category	6-26
6.7.4	Deleting Categories	6-26
6.7.5	Activating Categories	6-27
6.7.6	Deactivating Categories	6-27
6.8	Configuring the Registration Logic	6-27
6.9	Configuring the Answer Logic	6-29
6.9.1	About Answer Logic	6-30
6.9.2	Answer Logic Algorithms Examples	6-31
6.9.2.1	Abbreviations	6-31
6.9.2.2	Phonetics	6-31
6.9.2.3	Keyboard Fat Fingering	6-32
6.9.3	Level of Answer Logic	6-32
6.9.3.1	Abbreviation	6-32
6.9.3.2	Fat Fingering	6-33
6.9.3.3	Phonetics	6-33
6.9.3.4	Multiple Word Answers	6-33
6.10	Customizing English Abbreviations and Equivalences	6-34
6.11	Customizing Abbreviations and Equivalences for Locales	6-35
6.12	Setting Up a KBA Failure Counter	6-35
6.13	Use Cases	6-36
6.13.1	Use Case: Create Challenge Question	6-36
6.13.2	Use Case: KBA Registration Logic	6-37
6.13.3	Use Case: KBA Phone Challenge	6-37
6.14	KBA Guidelines and Recommended Requirements	6-38
6.14.1	Best Practices for Managing Questions	6-38
6.14.2	Guidelines for Designing Challenge Questions	6-39
6.14.3	Guidelines for Answer Input	6-39
6.14.4	Other Recommended Requirements	6-39

7 Enabling Challenge Questions

7.1	What is KBA?	7-1
7.2	Phased Approach for Registration	7-2
7.2.1	Phase 1 - No Registration	7-2
7.2.2	Phase 2 - Optional Registration	7-2
7.2.3	Phase 3 - Required Registration	7-3
7.3	Checklist for Enabling Challenge Questions	7-3
7.4	Ensuring that Base Policies are Installed	7-3
7.5	Ensuring KBA Properties/Default Properties are Set	7-3
7.6	Uploading Challenge Questions	7-4
7.7	Importing and Enabling Policies	7-4
7.8	Configuring Rules for Policies	7-4
7.9	Configuring the Challenge Question Answer Validation	7-4
7.10	Configuring the Answer Logic	7-4

8 Setting Up OTP Anywhere

8.1	Introduction and Concepts	8-1
8.1.1	Out-of-Band OTP Delivery	8-1

8.1.2	One Time Password (OTP).....	8-1
8.1.3	Registration.....	8-2
8.1.4	OTP Challenge	8-2
8.1.5	KBA vs. OTP.....	8-2
8.1.6	OTP Failure Counters.....	8-2
8.1.7	OTP Resets	8-3
8.1.7.1	Reset OTP Profile.....	8-3
8.1.7.2	Unlock a Customer	8-3
8.2	User Flow	8-3
8.3	Setting Up OTP Anywhere.....	8-3
8.3.1	Enabling OTP Profile Registration and Preference Setting	8-4
8.3.2	Setting Up the Contact Input Elements for OTP Registration Page.....	8-4
8.3.3	Configuring the OTP Challenge Types	8-5
8.3.4	Configuring OTP Delivery	8-6
8.4	Configuring OTP Presentation.....	8-6
8.4.1	Adding an OTP Device	8-6
8.4.2	Changing an OTP Device	8-7
8.5	Enabling OTP Challenge.....	8-7
8.6	Setting Up Failure Counter.....	8-7
8.7	OTP Case Management.....	8-8
8.7.1	Resetting OTP Profile.....	8-8
8.7.2	Unlocking User	8-8
8.7.3	OTP Case Details	8-9
8.8	Viewing OTP Performance Data	8-9

Part IV Managing Policy Configuration

9 Managing Policies, Rules, and Conditions

9.1	Introduction and Concepts.....	9-1
9.1.1	Policies.....	9-1
9.1.2	Rules	9-2
9.1.3	Conditions.....	9-2
9.1.4	Checkpoints	9-3
9.1.5	Groups.....	9-4
9.1.6	Actions and Action Groups.....	9-4
9.1.7	Alerts and Alert Groups	9-5
9.1.8	User Group Linking	9-5
9.1.9	Run Mode.....	9-5
9.1.10	Trigger Combinations and Triggers.....	9-5
9.1.11	Nested Policies	9-5
9.1.12	Evaluating a Policy within a Rule	9-6
9.1.13	Scores and Weight	9-6
9.1.14	Scoring Engine.....	9-6
9.1.15	Import Policies	9-6
9.1.16	Policy Type	9-6
9.2	Planning Policies.....	9-6

9.3	Overview of Creating a Policy	9-7
9.4	Navigating to the Policies Search Page.....	9-8
9.5	Searching for a Policy	9-9
9.6	Viewing a Policy or a List of Policies	9-10
9.7	Viewing Policy Details	9-10
9.8	Creating Policies.....	9-11
9.9	Linking Policy to All Users or a User ID Group.....	9-12
9.9.1	Linking a Policy to All Users.....	9-13
9.9.2	Linking a Policy to a Group	9-14
9.10	Editing a Policy's General Information.....	9-15
9.11	Adding a New Rule	9-16
9.11.1	Starting the Rule Creation Process	9-16
9.11.2	Specifying General Rule Information	9-17
9.11.3	Configuring Preconditions	9-18
9.11.4	Adding Conditions.....	9-18
9.11.5	Specifying Results for the Rule	9-18
9.11.6	Adding or Copying a Rule to a Policy	9-19
9.12	Working with Trigger Combinations	9-19
9.12.1	Specifying Trigger Combinations.....	9-21
9.12.2	Changing the Sequence of the Trigger Combination	9-22
9.12.3	Deleting a Trigger Combination.....	9-23
9.13	Deleting Policies.....	9-23
9.14	Copying a Rule to a Policy.....	9-23
9.15	Copying a Policy to Another Checkpoint	9-24
9.16	Exporting and Importing a Policy	9-24
9.16.1	Exporting a Policy.....	9-25
9.16.2	Importing a Policy	9-25
9.17	Navigating to the Rules Search Page	9-26
9.18	Searching for Rules	9-27
9.19	Viewing Rule Details.....	9-28
9.20	Editing Rules.....	9-29
9.20.1	Modifying the Rule's General Information.....	9-30
9.20.2	Specifying Preconditions	9-30
9.20.3	Specifying the Results for a Rule	9-31
9.21	Working with Scores and Weights	9-32
9.22	Deleting Rules.....	9-32
9.23	Searching Conditions	9-33
9.24	Importing Conditions.....	9-34
9.25	Adding Conditions to a Rule	9-34
9.26	Viewing the Condition Details of a Rule.....	9-36
9.27	Exporting a Condition.....	9-37
9.28	Editing Conditions.....	9-37
9.29	Changing the Order of Conditions in a Rule.....	9-37
9.30	Deleting Conditions.....	9-38
9.31	Deleting Conditions from a Rule	9-38
9.32	Use Cases.....	9-39
9.32.1	Use Case: Rule Exception Group.....	9-39

9.32.2	Use Case: Import Policy	9-39
9.32.3	Use Case: Create a Policy.....	9-40
9.32.4	Use Case: Add New Rule	9-41
9.32.5	Use Case: Link Group to Rule Condition.....	9-43
9.32.6	Use Case: Copy Rule	9-43
9.32.7	Use Case: Trigger Combination.....	9-44
9.32.8	Use Case: Trigger Combination and Rule Evaluation.....	9-46
9.32.9	Use Case: Configuring User Flow	9-47
9.32.10	Use Case: Edit Existing Security Policy	9-48
9.32.11	Use Case: Policy Set Scoring Engine	9-49
9.32.12	Use Case: Copy Policy.....	9-49
9.32.13	Use Case: Conditions: IP: Login Surge	9-50
9.32.14	Use Case: Canceling Rule Creation.....	9-53
9.32.15	Use Case: Disable Trigger Combinations.....	9-54
9.32.16	Use Case: Condition: Evaluate Policy	9-54
9.33	Best Practices	9-55
9.33.1	Adding or Editing Policies/Rules	9-55

10 Managing Groups

10.1	About Groups.....	10-1
10.2	Group Types	10-1
10.3	Group Usage.....	10-3
10.4	User Flows.....	10-3
10.5	Navigating to the Groups Search Page.....	10-4
10.6	Searching for a Group	10-5
10.7	Viewing Details about a Group	10-6
10.8	Group Characteristics.....	10-7
10.9	Creating a Group	10-8
10.9.1	Defining a Group	10-8
10.9.2	Adding Members to a Group.....	10-9
10.10	Creating a New Element/Member to Add to the Group (No Search and Filter Options)	10-11
10.11	Filtering an Existing List to Select an Element to Add to the Group (No Creation of a New Element)	10-11
10.11.1	Adding a City to a Cities Group	10-12
10.11.2	Adding a State to a States Group	10-12
10.11.3	Adding a Country to a Country Group.....	10-12
10.12	Searching for and Adding Existing Elements or Creating and Adding a New Element	10-13
10.12.1	Selecting an Element to Add as a Member to the Group.....	10-13
10.12.2	Creating an Element (Member) to Add to the Group	10-15
10.13	Adding Alerts to a Group	10-15
10.13.1	Selecting an Existing Alert to Add to the Alert Group	10-15
10.13.2	Creating a New Alert to Add to the Alert Group.....	10-16
10.14	Searching for and Adding Existing Elements.....	10-17
10.14.1	Selecting an Element to Add as a Member to the Group.....	10-17
10.14.2	Adding Actions to an Action Group.....	10-18

10.14.2.1	Selecting an Existing Action to Add to an Action Group	10-18
10.14.2.2	Creating a New Action to Add to an Action Group	10-19
10.15	Editing a Member of a Group	10-20
10.16	Removing Members of a Group	10-21
10.17	Removing a User from a User Group	10-21
10.18	Exporting and Importing a Group	10-21
10.18.1	Exporting a Group	10-21
10.18.2	Importing a Group	10-22
10.19	Deleting Groups	10-22
10.20	Updating a Group Directly	10-23
10.21	Use Cases	10-23
10.21.1	Use Case: Migration of Groups	10-23
10.21.2	Use Case: Create Alert Group and Add Members	10-23
10.21.3	Use Case: Remove User from Group	10-24
10.21.4	Use Case: Block Users from a Black-listed Country	10-26
10.21.5	Use Case: Company Wants to Block Users	10-26
10.21.5.1	Create Country Blacklist Policy (1): Create Fraudulent Country Policy and Rule	10-27
10.21.5.2	Create Country Blacklist Policy (2): Create Country Group	10-27
10.21.5.3	Create Country Blacklist Policy (3): Create Fraud High Alert Group	10-27
10.21.5.4	Create Country Blacklist Security Policy (4 of 5): Create Block Action Group	10-28
10.21.5.5	Create Country Blacklist Security Policy (5 of 5): Attach Groups to Fraudulent Country Rule	10-28
10.21.6	Use Case: Block Users from Certain Countries	10-28
10.21.7	Use Case: Allow Only Users from Certain IP Addresses	10-29
10.21.8	Use Case: Check Users from Certain Devices	10-29
10.21.9	Use Case: Monitor Certain Users	10-29
10.22	Best Practices	10-29

11 Managing the Policy Set

11.1	Introduction and Concepts	11-1
11.1.1	Policy Set	11-1
11.1.2	Action and Score Overrides	11-2
11.1.3	Before You Begin	11-2
11.2	Navigating to the Policy Set Details Page	11-2
11.3	Viewing Policy Set Details	11-3
11.4	Adding or Editing a Score Override	11-3
11.5	Adding or Editing an Action Override	11-4
11.6	Editing a Policy Set	11-6
11.7	Use Cases	11-6
11.7.1	Use Case: Policy Set - Overrides	11-6
11.7.2	Policy Set - Overrides (Order of Evaluation)	11-7
11.8	Best Practices for the Policy Set	11-8

12 Using the Scoring Engine

12.1	Concept of Scores	12-1
------	-------------------------	------

12.1.1	Score.....	12-1
12.1.2	Weight	12-1
12.1.3	Rule	12-2
12.1.4	Policy	12-2
12.1.5	Policy Type	12-2
12.1.6	Checkpoint.....	12-2
12.1.7	Policy Set	12-2
12.1.8	Scoring Engines.....	12-2
12.2	How Does Risk Scoring Work?.....	12-3
12.2.1	Score Propagation.....	12-4
12.2.2	Nested Policies	12-5
12.2.3	Scoring Override.....	12-6
12.2.4	Action and Alert Overrides.....	12-6
12.3	Score Calculations.....	12-6
12.3.1	Policy Score.....	12-6
12.3.1.1	Aggregate Score	12-6
12.3.1.2	Average Score	12-6
12.3.1.3	Maximum Score	12-6
12.3.1.4	Minimum Score.....	12-6
12.3.1.5	Weighted Average Score	12-6
12.3.1.6	Weighted Maximum Score.....	12-6
12.3.1.7	Weighted Minimum Score	12-6
12.3.2	Checkpoint Score	12-6
12.3.2.1	Average Score	12-7
12.3.2.2	Maximum Score	12-7
12.3.2.3	Minimum Score.....	12-7
12.3.2.4	Weighted Average Score	12-7
12.3.2.5	Weighted Maximum Score.....	12-7
12.3.2.6	Weighted Minimum Score	12-7
12.4	Best Practices	12-7

13 Managing System Snapshots

13.1	Concepts.....	13-1
13.1.1	Snapshots	13-1
13.1.2	Snapshot Storage.....	13-1
13.1.3	Snapshot Metadata	13-1
13.1.4	Backup	13-2
13.1.5	Restore	13-2
13.1.6	How Restore Works	13-3
13.2	Navigating to the System Snapshot Search Page	13-3
13.3	Searching for a Snapshot.....	13-3
13.4	Viewing Details of a Snapshot	13-4
13.5	Creating a Backup.....	13-5
13.5.1	Backing Up the Current System to the System Database	13-5
13.5.2	Backing Up the System Configuration in Database and File	13-5
13.5.3	Backing Up the Current System to a File	13-6
13.6	Restoring a Snapshot	13-6

13.6.1	Steps to Restore Selected Snapshot	13-6
13.6.2	Loading and Restoring a Snapshot	13-7
13.6.3	Snapshot Restore Considerations.....	13-7
13.6.3.1	Snapshot in Live System (Single Server).....	13-7
13.6.3.2	Snapshot Restore in Multi-Server System (Connected to the Same Database)	13-7
13.6.3.3	Snapshot Restore in Multi-Server Running Different Versions.....	13-7
13.7	Deleting a Snapshot.....	13-7
13.8	Limitations of Snapshots.....	13-7
13.9	Diagnostics.....	13-8
13.10	Use Cases.....	13-8
13.10.1	System Snapshot Import/Export	13-8
13.10.2	Use Case: User Exports Policy Set as a Record for Research.....	13-8
13.10.3	Use Case: User Replaces Entire System.....	13-8
13.10.4	Use Case: User Identifies Policy Set to Import	13-9
13.11	Best Practices for Snapshots	13-9

Part V Autolearning

14 Managing Autolearning

14.1	Introduction and Concepts.....	14-1
14.1.1	Autolearning.....	14-1
14.1.2	Patterns.....	14-1
14.1.3	Member Types and Attributes.....	14-3
14.1.4	Buckets	14-3
14.1.5	Pattern Rules Evaluations.....	14-6
14.1.6	Bucket Population	14-8
14.2	Quick Start for Enabling Autolearning for Your System	14-8
14.3	Before You Begin.....	14-9
14.3.1	Importing Basic Authentication-Related Entities	14-9
14.3.2	Enabling Autolearning Properties.....	14-9
14.3.3	Using Autolearning in Native Integration.....	14-10
14.4	User Flows.....	14-10
14.4.1	Creating a New Pattern	14-10
14.4.2	Editing a Pattern	14-11
14.5	Navigating to the Patterns Search Page.....	14-11
14.6	Searching for a Pattern	14-11
14.7	Navigating to the Patterns Details Page.....	14-14
14.8	Viewing Pattern Details	14-14
14.8.1	Viewing Details of a Specific Pattern.....	14-14
14.9	Creating and Editing Patterns.....	14-14
14.9.1	Creating a Pattern	14-14
14.9.2	Adding Attributes.....	14-17
14.9.3	Activating and Deactivating Patterns.....	14-18
14.9.3.1	Activating Patterns.....	14-19
14.9.3.2	Deactivating Patterns.....	14-19
14.9.4	Editing the Pattern.....	14-19
14.9.5	Changing the Status of the Pattern.....	14-20

14.9.6	Adding or Changing Member Types.....	14-20
14.9.7	Changing the Evaluation Priority	14-21
14.9.8	Editing Attributes	14-21
14.9.9	Deleting Attributes	14-21
14.10	Importing and Exporting Patterns	14-21
14.10.1	Importing Patterns.....	14-21
14.10.2	Exporting Patterns.....	14-22
14.11	Deleting Patterns.....	14-22
14.12	Using Autolearning Data/Profiling Data	14-22
14.12.1	Create a Policy that Uses Autolearning Conditions	14-23
14.12.2	Associate Autolearning Condition with Policy.....	14-23
14.12.3	Check Session Details.....	14-23
14.13	Use Cases.....	14-23
14.13.1	Use Case: Challenge Users If Log In Different Time Than Normally	14-23
14.13.2	Use Case: Test a Pattern.....	14-24
14.13.3	Use Case: Track Off-Hour Access	14-24
14.13.4	Use Case: User Logs in During a Certain Time of Day More Than X Times	14-26
14.13.5	Use Case: Patterns Can have Multiple Member Types	14-26
14.13.6	Use Case: City Usage	14-27
14.13.7	Use Case: Autolearning Adapts to Behavior of Entities	14-28
14.13.8	Use Case: Single Bucket Pattern	14-29
14.13.9	Use Case: Using Pattern.....	14-30
14.14	Pattern Attributes Operators Reference	14-32
14.14.1	For Each.....	14-33
14.14.2	Equals	14-33
14.14.3	Less Than	14-33
14.14.4	Greater Than.....	14-33
14.14.5	Less Than Equal To.....	14-33
14.14.6	Greater Than Equal To.....	14-33
14.14.7	Not Equal	14-34
14.14.8	In.....	14-34
14.14.9	Not In.....	14-34
14.14.10	Like.....	14-34
14.14.11	Not Like.....	14-34
14.14.12	Range	14-34
14.14.12.1	Fixed Range	14-35
14.14.12.2	Fixed Range with Steps (or Increment)	14-35
14.14.12.3	Upper Unbound Ranges with Steps	14-36

15 Managing Configurable Actions

15.1	Introduction and Concepts.....	15-1
15.1.1	Configurable Actions	15-1
15.1.2	Action Templates	15-1
15.1.3	Deploying a Configurable Action	15-2
15.2	Creating Configurable Actions	15-3
15.2.1	Define New Action Template	15-3
15.2.2	Use Existing Action Template.....	15-3

15.2.3	Create Action Instance	15-3
15.3	Navigating to the Action Templates Search Page	15-4
15.4	Searching for Action Templates.....	15-4
15.5	Viewing Action Template Details.....	15-5
15.6	Creating a New Action Template	15-5
15.7	Navigating to the Action Instances Search Page.....	15-7
15.8	Searching for Action Instances.....	15-8
15.9	Creating an Action Instance and Adding it to a Checkpoint	15-8
15.10	Creating a Custom Action Instance.....	15-11
15.11	Editing an Action Template.....	15-12
15.12	Exporting Action Templates.....	15-12
15.13	Importing Action Templates	15-12
15.14	Moving an Action Template from a Test Environment	15-12
15.15	Deleting Action Templates	15-13
15.16	Viewing a List of Configurable Action Instances.....	15-13
15.17	Viewing the Details of an Action Instance	15-13
15.18	Editing an Action Instance.....	15-13
15.19	Deleting an Existing Action Instance	15-14
15.20	Out-of-the-Box Configurable Actions	15-14
15.20.1	Defining CaseCreationAction	15-14
15.20.2	Defining AddItemtoListAction.....	15-15
15.21	Use Cases.....	15-16
15.21.1	Use Case: Add Device to Black List	15-16
15.21.2	Use Case: Add Device to Watch-list Action.....	15-16
15.21.3	Use Case: Custom Configuration Action	15-17
15.21.4	Use Case: Create Case	15-18

Part VI Managing Transactions

16 Creating and Managing Entities

16.1	Introduction and Concepts.....	16-1
16.1.1	Entities.....	16-1
16.1.2	Data Elements.....	16-1
16.1.3	Display Element	16-2
16.1.4	ID Scheme	16-2
16.1.5	Internal ID.....	16-2
16.1.6	External ID.....	16-2
16.2	Navigating to the Entities Search Page.....	16-2
16.3	Searching for Entities.....	16-3
16.4	Creating an Entity	16-4
16.4.1	Initial Steps	16-4
16.4.2	Adding and Editing Data Elements	16-5
16.4.3	Selecting Elements for the ID Scheme	16-6
16.4.4	Specifying Data for the Display Scheme	16-8
16.4.5	Activating the Entity	16-9
16.5	Viewing Details of a Specific Entity	16-9
16.6	Editing the Entity	16-10

16.7	Exporting Entities	16-10
16.8	Importing Entities.....	16-11
16.9	Activating Entities.....	16-11
16.10	Deactivating Entities.....	16-11
16.11	Deleting Entities.....	16-12
16.12	Re-ordering the Rows in the ID Scheme and Display tabs.....	16-12
16.13	Best Practices	16-12

17 Managing Transactions

17.1	Introduction and Concepts.....	17-1
17.1.1	Transactions.....	17-1
17.1.2	Entities.....	17-1
17.1.3	Transaction Data	17-2
17.1.4	Transaction Handling	17-2
17.2	Overview of Defining and Using Transaction Definition.....	17-2
17.3	Navigating to the Transactions Search Page.....	17-4
17.4	Searching for a Transaction Definition	17-5
17.5	Viewing Transaction Definitions	17-5
17.6	Prerequisites for Using Transactions	17-5
17.7	Creating the Transaction Definition	17-6
17.8	Adding an Existing Entity to the Transaction	17-6
17.9	Creating a New Entity and Adding It to the Transaction.....	17-7
17.10	Defining Transaction Data for the Transaction at the Oracle Adaptive Access Manager End 17-7	
17.11	Defining Parameters for the Transaction from the Client's End.....	17-8
17.12	Mapping the Source Data	17-9
17.12.1	Mapping Transaction Data to the Source Data	17-9
17.12.2	Mapping Entities to the Source Data	17-10
17.12.3	Editing Mapping.....	17-10
17.13	Activating the Transaction Definition	17-10
17.14	Editing a Transaction Definition.....	17-11
17.15	Exporting Transaction Definitions	17-11
17.16	Importing Transaction Definition.....	17-12
17.17	Activating a Transaction Definition	17-12
17.18	Deactivating a Transaction Definition	17-12
17.19	Deleting Transaction Definitions.....	17-13
17.20	Use Cases.....	17-13
17.20.1	Implementing a Transaction Use Case	17-13
17.20.2	Use Case: Transaction Frequency Checks.....	17-15
17.20.3	Use Case: Transaction Frequency and Amount Check against Suspicious Beneficiary Accounts 17-15	
17.20.4	Use Case: Transaction Check against Blacklisted Deposit and Beneficiary Accounts	17-15
17.20.5	Use Case: Transaction Pattern	17-16
17.20.6	Use Case: Composite or Nested Transactions	17-17

Part VII Reporting

18 Using the Dashboard

18.1	Introduction	18-1
18.1.1	What is a Dashboard?	18-1
18.1.2	Common Terms and Definitions	18-1
18.2	Navigation.....	18-2
18.3	Using the Dashboard in Oracle Adaptive Access Manager	18-2
18.3.1	Performance.....	18-2
18.3.1.1	Viewing Statistics in Total View and Trending View	18-2
18.3.1.2	Viewing Performance Data	18-3
18.3.1.3	Difference Between Performance Panel and Performance Dashboard	18-3
18.3.2	Summary	18-4
18.3.3	Dashboards.....	18-5
18.3.3.1	Viewing Data Type by Location.....	18-6
18.3.3.2	Viewing a List of Scoring Breakdowns	18-7
18.3.3.3	Security Dashboard	18-7
18.3.3.4	Viewing a List of Rules or Alerts by Security.....	18-7
18.3.3.5	Viewing Browser and Operating System Data by Device	18-8
18.3.3.6	Viewing a Data Type by Performance.....	18-8
18.3.3.7	Using the Total and Trending Views.....	18-9
18.3.3.8	Viewing the Trending View Graph	18-9
18.3.3.9	View by Range	18-10
18.3.3.10	View by Sample	18-10
18.3.3.11	Last Updated	18-10
18.3.3.12	Using Tooltips.....	18-10
18.4	Use Cases.....	18-10
18.4.1	Use Case: Trend Rules Performance on Dashboard	18-10
18.4.2	Use Case: View Current Activity.....	18-11
18.4.3	Use Case: View Aggregate Data.....	18-12
18.4.4	Use Cases: Additional Security Administrator and Fraud Investigator Use Cases.....	18-12
18.4.5	Use Cases Additional Business Analyst Use Cases	18-13

19 Configuring BI Publisher Reports

19.1	Setting up Oracle Business Intelligence Publisher for Oracle Adaptive Access Manager Reports 19-1	
19.1.1	Installing BI Publisher.....	19-1
19.1.2	Installing Oracle Adaptive Access Manager BI Publisher Reports	19-1
19.1.3	Configuring Oracle Adaptive Access Manager BI Publisher Reports	19-2
19.1.4	Testing Oracle Adaptive Access Manager BI Publisher Configuration	19-3
19.2	Viewing/Running Reports.....	19-3
19.3	Scheduling a Report.....	19-4
19.4	Example Report Scenarios	19-5
19.4.1	Example General Nightly Report	19-5
19.4.1.1	User/Recent Logins	19-5
19.4.1.2	Device details	19-5
19.4.1.3	Device/Multiple Failures	19-6
19.4.1.4	User/Recent Logins	19-6

19.4.1.5	Location details	19-6
19.4.1.6	Location/Users by Location	19-6
19.4.2	Additional Sample Analyses.....	19-7
19.4.2.1	Here are some example values that could be used.....	19-7
19.4.2.2	Device/ Users by Device	19-7
19.5	Best Practices for Creating Reports	19-7
19.6	Use Cases.....	19-8
19.6.1	Use Case: BIP Reports	19-9
19.6.1.1	Description	19-9
19.6.1.2	Steps.....	19-9

20 Monitoring Performance by Using Fusion Middleware Control

20.1	Displaying Fusion Middleware Control.....	20-1
20.2	Displaying Base Domain 11g Farm Page.....	20-2
20.3	Oracle Adaptive Access Manager Cluster Home Page	20-4
20.4	Oracle Adaptive Access Manager Server Home Page.....	20-6

21 Monitor and Audit of Events

21.1	Monitoring Information Sent to Dynamic Monitoring System.....	21-1
21.1.1	Login Information (Counts Only)	21-1
21.1.2	Rules Engine Execution Information (Count and Time Taken to Execute)	21-1
21.1.3	APIs Execution Information (Count and Time Taken to Execute)	21-2
21.2	Audit Information Sent to Audit System	21-2
21.2.1	Customer Care Events.....	21-2
21.2.2	Policy Management Events	21-2
21.2.3	KBA Questions Events	21-3
21.2.4	Group/List Management Events	21-4

Part VIII Deployment Management

22 Using the Properties Editor

22.1	Navigating to the Properties Search Page	22-1
22.2	Searching for a Property	22-2
22.3	Viewing the Value of a Property	22-3
22.4	Viewing Enumerations.....	22-3
22.5	Creating a New Database Type Property	22-3
22.6	Editing the Values for Database and File Type Properties	22-3
22.7	Deleting Database Type Properties	22-4
22.8	Exporting Database and File Type Properties	22-4
22.9	Importing Database Type Properties	22-4

Part IX Command-Line Interface

23 Oracle Adaptive Access Manager Command-Line Interface Scripts

23.1	CLI Overview	23-1
------	--------------------	------

23.2	Setting Up the CLI Environment	23-1
23.2.1	Set up the CLI Work Folder	23-1
23.2.2	Set Up the Credential Store Framework (CSF).....	23-2
23.2.2.1	Use CSF without MBeans	23-2
23.2.2.2	Use CSF with MBeans	23-3
23.2.3	Set the Oracle Adaptive Access Manager Database Credentials in the Credential Store Framework 23-4	
23.3	Using CLI	23-5
23.3.1	Obtaining Usage Information for Import or Export	23-5
23.3.2	Command-Line Options	23-5
23.3.2.1	What is the Syntax for Commands?.....	23-5
23.3.2.2	CLI Parameters	23-6
23.3.2.3	Supported Modules for Import and Export.....	23-6
23.3.2.4	Import of Files	23-7
23.3.2.5	Export of Files	23-8
23.3.2.6	Import Options	23-10
23.3.2.7	Importing Multiple Types of Entities in One Transaction	23-10
23.3.2.8	Multiple Modules and Extra Options (Common vs. Specific).....	23-11
23.3.2.9	Transaction Handling	23-11
23.3.2.10	Upload Location Database	23-12
23.3.3	Globalization	23-12
23.4	Importing IP Location Data	23-12
23.4.1	Loading the Location Data to the Oracle Adaptive Access Manager Database....	23-12
23.4.1.1	Setting Up for SQL Server Database.....	23-12
23.4.1.2	Setting Up IP Location Loader Properties	23-12
23.4.1.3	Setting Up for Loading MaxMind IP data	23-13
23.4.1.4	Setting Up Encryption	23-13
23.4.1.5	Loading Location Data	23-13
23.4.2	System Behavior.....	23-14
23.4.3	Quova File Layout	23-14
23.4.3.1	Routing Types Mapping.....	23-15
23.4.3.2	Connection Types Mapping.....	23-16
23.4.3.3	Connection Speed Mapping.....	23-17
23.4.4	Oracle Adaptive Access Manager Tables.....	23-18
23.4.4.1	Anonymizer.....	23-18
23.4.4.2	Tables in Location Loading.....	23-18
23.4.5	Verifying When the Loading was a Success	23-19

Part X Multitenancy

24 Multitenancy

24.1	Multitenancy Scenario.....	24-1
24.2	Changes in Terminology.....	24-2
24.3	Mapping of Application ID (Client-Side) to Organization ID (Administration Side)...	24-3
24.4	Multitenant Support In Oracle Adaptive Access Manager	24-4

Part XI Troubleshooting

25 Troubleshooting

25.1	Import/Export.....	25-1
25.2	Transactions.....	25-2
25.3	Globalization.....	25-2
25.4	Case Management.....	25-2
25.5	KBA.....	25-4
25.6	Database.....	25-5
25.7	Localization.....	25-5
25.8	Policies, Rules, and Conditions.....	25-6
25.9	Groups.....	25-7
25.10	Configurable Actions.....	25-9
25.11	Autolearning.....	25-10
25.12	Entities.....	25-10
25.13	Time Zones.....	25-11
25.14	Dashboard.....	25-12
25.15	Command-Line Interface.....	25-13
25.16	Location Loader.....	25-13
25.17	Encryption.....	25-14
25.18	Monitoring Performance.....	25-14
25.19	Audit and Query.....	25-15

Part XII Appendixes

A Pattern Processing

A.1	Pattern Data Processing.....	A-1
A.2	APIs for Triggering Pattern Data Processing.....	A-2
A.2.1	updateTransaction.....	A-2
A.2.2	updateAuthStatus.....	A-3
A.2.3	processPatternAnalysis.....	A-3

B Conditions Reference

B.1	Descriptions.....	B-6
B.1.1	Device Conditions.....	B-6
B.1.1.1	Device: Browser header substring.....	B-7
B.1.1.2	Device: Device firsttime for user.....	B-7
B.1.1.3	Device: In Group.....	B-8
B.1.1.4	Device: Excessive Use.....	B-8
B.1.1.5	Device: Is registered.....	B-9
B.1.1.6	Device: User count.....	B-10
B.1.1.7	Device: Timed not status.....	B-10
B.1.1.8	Device: Used count for User.....	B-11
B.1.1.9	Device: Velocity from last login.....	B-12
B.1.2	Autolearning Conditions.....	B-13
B.1.2.1	Entity: Entity is Member of Pattern Bucket for the first time in Certain Time Period B-13	
B.1.2.2	Entity: Entity is member of pattern less than some percent times.....	B-14

B.1.2.3	Entity: Entity is member of pattern bucket less than some percent with all entities in picture	B-15
B.1.2.4	Entity: Entity is member of pattern N times	B-16
B.1.2.5	Entity: Entity is member of bucket N times in a given time period.....	B-17
B.1.3	Location Conditions	B-19
B.1.3.1	Location: ASN in group	B-20
B.1.3.2	Location: IP in Range group	B-20
B.1.3.3	Location: In Country group	B-21
B.1.3.4	Location: IP Connection type in group	B-22
B.1.3.5	Location: IP line speed type	B-22
B.1.3.6	Location: IP Routing Type in group	B-23
B.1.3.7	Location: In carrier group	B-23
B.1.3.8	Location: IP Maximum Users	B-24
B.1.3.9	Location: Is IP from AOL	B-25
B.1.3.10	Location: in city group	B-25
B.1.4	Transactions Conditions	B-26
B.1.4.1	Transaction: Check Current Transaction Using Filter Condition.....	B-26
B.1.4.2	Transaction: Check Transaction Count Using Filter Condition	B-27
B.1.4.3	Transaction: Check Transaction Aggregate and Count Using Filter Conditions.....	B-31
B.1.4.4	Transaction: Check Count of any entity or element of a Transaction using filter conditions	B-35
B.1.4.5	Transaction: Check if consecutive Transactions in given duration satisfy the filter conditions	B-37
B.1.4.6	Transaction: Compare Transaction Aggregates (Sum/Avg/Min/Max) across two different durations	B-39
B.1.4.7	Transaction: Compare Transaction counts across two different durations	B-41
B.1.4.8	Transaction: Compare Transaction Entity/Element counts across two different durations	B-42
B.1.5	In-Session Conditions.....	B-44
B.1.5.1	Session: Check Param Value	B-44
B.1.5.1.1	Parameters.....	B-44
B.1.5.1.2	Possible User Scenarios	B-45
B.1.5.2	Session: Check param value for regex	B-45
B.1.5.2.1	Parameters.....	B-46
B.1.5.2.2	Possible User Scenarios	B-47
B.1.5.3	Session: Check param value in group	B-47
B.1.5.4	Session: Check String Value.....	B-49
B.1.5.4.1	Parameters.....	B-49
B.1.5.4.2	Possible User Scenarios	B-49
B.1.5.5	Session: Time Unit Condition	B-49
B.1.6	System Conditions	B-51
B.1.6.1	System - Check Boolean Property	B-52
B.1.6.1.1	Parameters.....	B-52
B.1.6.1.2	Possible User Scenarios	B-52
B.1.6.2	System - Check Int Property	B-52
B.1.6.3	System - Check String Property.....	B-53
B.1.6.4	System - Check Request Date	B-54

B.1.7	User Conditions	B-55
B.1.7.1	User: Check User Data	B-55
B.1.7.2	User: Stale Session	B-56

C Oracle Adaptive Access Manager Reports Reference

C.1	Common Reports	C-1
C.2	Devices Reports	C-1
C.3	KBA Reports	C-1
C.4	Location Reports	C-2
C.5	Performance Reports	C-2
C.6	Security Reports	C-2
C.7	Summary Reports	C-3
C.8	Users Reports.....	C-3

D Oracle Adaptive Access Manager Properties

D.1	Properties	D-1
D.2	OTP Properties	D-3
D.3	Time Zone	D-4

E The Discovery Process

E.1	Discovery Process Overview.....	E-1
E.2	Example Scenario: Transaction Security.....	E-1
E.2.1	Problem Statement.....	E-1
E.2.2	Inputs Available.....	E-1
E.2.3	Evaluation	E-2
E.2.4	Outcomes	E-2
E.2.5	Translation	E-2
E.2.6	Alert	E-2
E.3	Example Scenario: Login Security	E-2
E.3.1	Problem Statement.....	E-2
E.3.2	Inputs Available.....	E-3
E.3.3	Evaluation.....	E-3
E.3.4	Outcome	E-3
E.3.5	Translation	E-3
E.3.6	Action	E-4

F Globalization Support

F.1	Supported Languages	F-1
F.2	Turning Off Localization	F-1
F.3	Configuring Language Defaults for Oracle Adaptive Access Manager	F-1
F.3.1	Example 1	F-2
F.3.2	Example 2.....	F-3
F.3.3	Example 3.....	F-4
F.4	Dashboard	F-4
F.5	Answer Logic Phonetics Algorithms	F-4

F.6	Keyboard Fat Fingering	F-5
F.7	Adding Registration Questions	F-5
F.8	Adding Abbreviations and Equivalences for Answer Logic.....	F-5

G Setting Up Archive and Purge Procedures

G.1	Purge Process.....	G-1
G.2	Archive Process	G-1
G.3	Database Archive and Purge.....	G-1
G.3.1	Archive and Purge Data Classification.....	G-1
G.3.1.1	Device Fingerprinting.....	G-1
G.3.1.2	Transaction In-Session Based Data	G-2
G.3.1.3	Autolearning Profile Data	G-2
G.3.1.4	Rule Log Data.....	G-2
G.3.2	Archive and Purge Process.....	G-3
G.3.2.1	Archive and Purge Process - Special Recommendations for Schemas with Partitioned Objects G-3	
G.3.2.1.1	Schema with Partitioned Objects (Oracle Databases Only) Without a Separate Reporting Database G-3	
G.3.2.1.2	Schema with Partitioned Objects (Oracle Databases Only) With a Separate Reporting Database G-3	
G.3.2.2	Archive and Purge Process - Setting Up for Users with an Existing Process In Place G-3	
G.3.2.3	Archive and Purge Process - Setting Up for the Oracle Database.....	G-4
G.3.2.3.1	Prerequisite.....	G-4
G.3.2.3.2	Instructions.....	G-4
G.3.3	Performing Archive and Purge.....	G-5
G.3.3.1	Manual Execution.....	G-5
G.3.3.2	Automatic Scheduling	G-6
G.3.4	Validating Archive and Purge	G-6
G.3.5	Restoring Archived Data	G-6
G.3.6	Archive and Purge Details	G-6
G.3.6.1	Device Fingerprint Tables and Corresponding Archived Tables.....	G-6
G.3.6.2	Autolearning Transactional Tables and Corresponding Archive Tables.....	G-6
G.3.6.3	Transaction Tables and Corresponding Archived Tables	G-7
G.3.6.4	Rule Logs Tables and Corresponding Archived Tables	G-7
G.3.7	Scripts to Set Up Archive and Purge	G-7
G.3.7.1	Scripts for the Oracle Database.....	G-7
G.3.7.1.1	create_purge_proc.sql.....	G-7
G.3.7.2	Scripts to Execute Archive and Purge	G-8
G.3.7.2.1	exec_sp_purge_tracker_data.sql	G-8
G.3.7.2.2	exec_sp_purge_txn_log.sql	G-9
G.3.7.2.3	exec_sp_purge_workflow_data.sql	G-9
G.3.7.2.4	exec_sp_purge_profile_data.sql	G-9
G.3.7.2.5	exec_sp_purge_rule_log.sql.....	G-9
G.3.7.3	Drop Scripts for Partitioned Tables	G-10
G.3.7.3.1	Drop_Monthly_Partition_tables.sql	G-10
G.3.7.3.2	Drop_Weekly_Partition_tables.sql	G-10
G.4	Case Data Archive and Purge	G-10

G.4.1	Archive and Purge Process for Case Data.....	G-10
G.4.1.1	Set Up the Archive and Purge Script.....	G-10
G.4.1.1.1	Prerequisite.....	G-11
G.4.1.1.2	Set Up Archive and Purge Script	G-11
G.4.1.2	Execute Archive and Purge Script	G-11
G.4.1.2.1	Manual Execution.....	G-12
G.4.1.2.2	Automatic Scheduling	G-12
G.4.1.3	Validating Archive and Purge	G-12
G.4.1.4	Restoring Archived Data	G-12
G.4.1.5	Case Data Archive and Purge Details	G-12
G.4.1.5.1	Case-Related Tables and Their Corresponding Archived Tables	G-12
G.4.1.5.2	create_case_purge_proc.sql - Setup Script for Archive and Purge	G-13
G.4.1.5.3	exec_purge_case_data.sql - Execution Script for Archive and purge execution script G-13	
G.5	Monitor Data Archive and Purge	G-13
G.5.1	Archive and Purge Process for Monitor Data.....	G-13
G.5.1.1	Set Up the Archive and Purge Script.....	G-14
G.5.1.1.1	G-14
G.5.1.1.2	Prerequisite - Privileges Granted to Schema	G-14
G.5.1.1.3	Set Up Archive and Purge Instructions	G-14
G.5.1.2	Execute Archive and Purge Script	G-15
G.5.1.2.1	Manual Execution.....	G-15
G.5.1.2.2	Automatic Scheduling	G-16
G.5.1.3	Validating Archive and Purge	G-16
G.5.1.4	Restoring Archived Data	G-16
G.5.1.5	Monitor Data Archive and Purge Details	G-16
G.5.1.5.1	Monitor Data-Related Table and the Corresponding Archived Table.....	G-16
G.5.1.5.2	create_v_monitor_purge_proc.sql - Setup Script for Archive and Purge..	G-16
G.5.1.5.3	exec_v_monitor_purge_proc.sql - Execution Script for Archive and purge execution script G-17	

H Configuring Logging Output

H.1	Handlers.....	H-1
H.1.1	Configuring the File handler.....	H-1
H.1.2	Configuring Both Console Logging and File Logging	H-2
H.2	Oracle Adaptive Access Manager Loggers	H-2
H.3	Logging Levels	H-2
H.4	Other Properties	H-3

I Rule and Fingerprint Logging

I.1	Detailed Rule Logging.....	I-1
I.1.1	Enabling Detailed Rule Logging	I-1
I.1.2	Specifying When to Log.....	I-1
I.1.3	Configuring Detailed Logging Threshold Time.....	I-2
I.1.4	Rule Logging Flow	I-2
I.1.5	Value Combinations	I-3

1.1.6	Logging Non-Triggered Rules	1-3
1.1.6.1	Examples	1-3
1.2	Enabling Fingerprint Rule Logging	1-4
1.3	Specifying Properties in Running Both Fingerprint and Detailed Logging.....	1-4

Index

Preface

The *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager* provides in-depth information for the following tasks:

- Using the dashboard for online monitoring and investigation, monitoring alerts, and running queries
- Using the set of customer care tools to create cases and support Customer Service Representatives (CSR). The cases record all the actions performed by a CSR to assist the user as well as various account activities of the user
- Using knowledge-based authentication 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
- Setting up OTP Anywhere to 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 in a few easy steps
- Setting up a Policy Set to evaluate traffic and to identify possible risks at checkpoints
- Creating and managing policies, which contain security rules and configurations used to evaluate the level of risk at each checkpoint.
- Creating groups to be used in rule conditions, to link a policy to user groups, as alert and action groups, and as exceptions groups.
- Configuring patterns to record the behavior of the user accessing the system and to profile (creates a digest of) the user's data
- Managing supplementary actions that are triggered based on the result action, or based on the risk scoring after a checkpoint execution, or based on both
- Managing entities, user-defined structure that can be re-used across different transactions
- Mapping client-specific transactions with corresponding entities so information can be captured and used for enforcing authorization rules, fraud analysis, and so on
- Using Oracle BI Publisher as the reporting solution for Oracle Adaptive Access Manager

Audience

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

Users	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.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

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

Related Documents

For more information, see the following documents in the Oracle 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*
- *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.
<i>italic</i>	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 11g Release 1 (11.1.1)?

This chapter introduces the new and changed administrative features of Oracle Adaptive Access Manager 11g 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 11g Release 1 (11.1.1)

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

Areas	Features and Enhancements
Interface	<p>The new rich Oracle Adaptive Access Manager user interface provides</p> <ul style="list-style-type: none">▪ Navigation and Policy trees, which allow quick and visible access to features▪ Tabs and accordion panels that reduce real estate usage for multitasking.▪ Streamlined flows that capture use case flows of execution. For example, the flow for rules is search, create, edit, and copy rules.▪ Improved search and filtering, where you can save searches and filter directly on columns▪ New and improved screens in Oracle Adaptive Access Manager. Oracle Adaptive Access Manager provides enhanced usability for fraud analysis and forensic operations▪ Advanced table display controls to add and remove columns, reposition and resize columns, and detach columns▪ Direct access to documentation from Oracle Adaptive Access Manager

Areas	Features and Enhancements
Policy Creation	<p>New features in policy creation enables you to:</p> <ul style="list-style-type: none"> ■ Copy policies to checkpoints 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. ■ Configure trigger combinations more easily The new design enables you to more easily define and manage trigger combinations and allows the appending or overriding of actions and alerts. ■ Execute nested conditions New conditions support the execution of nested policies. ■ View indicators 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	<p>Rules are now much easier to create.</p> <ul style="list-style-type: none"> ■ Rule creation has been simplified with the removal of rule templates from the product. ■ Rules can be copied to different policies under any checkpoint
OTP Anywhere	<p>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.</p>
Encryption Keys	<p>Encryption keys required by Oracle Adaptive Access Manager can be securely managed using Fusion Middleware Control without having to create Keystore files.</p>
Universal Risk Snapshot	<p>Snapshots can be created allowing security administrators to simply and easily migrate security data across environments or restore security configuration to a known state.</p>
Audit	<p>Most of the administrative operations are now audited using Oracle Audit Service. Audit events can be viewed using the standard audit reports.</p>
Web Services	<p>Oracle Adaptive Access Manager Web services are implemented using Oracle Web Services.</p>
Application Logging	<p>Oracle Adaptive Access Manager 11g uses Java logging instead of log4j. Logging can be configured using Fusion Middleware Control.</p>
Integration with the Dynamic Monitoring System	<p>Some performance metrics are now integrated with Dynamic Monitoring System. These metrics and related reports can be viewed using Fusion Middleware Control</p>

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

Features	10.1.4.3	10.1.4.5	11gR1
Real-time and offline rules engine	X	X	X
Virtual authentication devices	X	X	X

Features	10.1.4.3	10.1.4.5	11gR1
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
Common audit framework			X
Integrated Oracle Identity Manager password management flows			X
Oracle Installer and Repository Creation Utility			X
Oracle Patch			X
Oracle Adaptive Access Manager Offline User Interface	X	X	
Document Models	X	X	
Globalization		X	X
Integrations	10.1.4.3	10.1.4.5	11gR1
Oracle Access Manager integration	X	X	X
Oracle Identity Manager integration			X
Oracle Entitlements Server integration		X	X
Juniper SSL VPN integration		X	X

Note: Oracle Adaptive Access Manager "offline" risk analysis functionality is available in 10g (10.1.4.5). Oracle Adaptive Access Manager 11gR1 customers can deploy 10g in their offline environment. This is possible since Oracle Adaptive Access Manager 10g and 11g use the same schema. For information on Oracle Adaptive Access Manager Offline, see the 10g (10.1.4.5) guides.

Concepts and Terminology Changes for Oracle Adaptive Access Manager 11g

Customers migrating from Oracle Adaptive Access Manager 10g to 11gR1 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

10g Term	11g Term
runtime	checkpoint
model	policy
manual override	trigger combination
Application ID	<p>Organization ID</p> <p>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.</p> <p>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.</p>

Concept Changes

Concepts changes are listed in the following table.

10g Concept	11gR1 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 11g 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 Oracle Adaptive Access Manager 11g 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"](#)
- [Chapter 3, "Oracle Adaptive Access Manager Navigation"](#)

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. Oracle Adaptive Access Manager provides risk-aware authentication, real-time behavior profiling, and transaction and event risk analysis.

Oracle Adaptive Access Manager contains functionality in 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	<p>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.</p> <p>Functionality that support risk analysis are:</p> <ul style="list-style-type: none"> ■ Rules Engine ■ Entities ■ Transactions ■ Patterns ■ Alerts ■ Actions ■ Configurable actions
End-user facing functionality to prevent fraud	<p>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.</p> <p>Functionality that supports end-user facing security are:</p> <ul style="list-style-type: none"> ■ Virtual authentication devices ■ Knowledge-Based Authentication (KBA) ■ OTP Anywhere ■ Security policies

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

- [Benefits of Oracle Adaptive Access Manager](#)
- [Oracle Adaptive Access Manager Features](#)
- [Oracle Adaptive Access Manager User Roles](#)
- [Oracle Adaptive Access Manager Integrations](#)
- [Oracle Adaptive Access Manager Architecture](#)

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

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 used for fraud monitoring and detection.

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.

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 User Roles

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

Table 1–2 Oracle Adaptive Access Manager User Roles

Role	Description
Security Investigators and Customer Service Representatives	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. Analysts work with security investigators and CSRs to identify the policies that require adjustment and new policies that need to be created.
Business/Security Analyst	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.
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.

1.4 Oracle Adaptive Access Manager Integrations

This section provides a brief summary for the following integrations:

- [Native Integration](#)
- [Reverse Proxy Integration](#)
- [Access Management Integration](#)
- [SAML Integration](#)

1.4.1 Native Integration

The server portion of Oracle Adaptive Access Manager can be natively integrated with a web application. In the native integration, the application invokes the Oracle Adaptive Access Manager APIs directly to access risk and challenge flows.

The two flavors of native integration are:

- SOAP/Web Services Integration
 - The web application communicates with OAAM Admin using the Oracle Adaptive Access Manager Native Client API or through Web Services.
- Static Linked (In Proc) Integration
 - The native integration involves only local API calls and therefore no remote server risk engine calls. The integration embeds the processing engine for OAAM Admin

with the application and enables it to leverage the underlying database directly for processing.

Both flavors use the same APIs, but during a checkpoint, the appropriate option can be chosen by configuring the properties.

1.4.2 Reverse Proxy Integration

The Oracle Adaptive Access Manager reverse proxy option is a proxy-based deployment of the OAAM Admin and OAAM Server that requires little or no integration with enterprise applications.

A proxy intercepts site traffic and routes it through OAAM Admin for strong authentication and fraud detection and prevention.

1.4.3 Access Management Integration

Oracle Adaptive Access Manager is integrated or used along with an access management product. This option uses both OAAM Server and OAAM Admin applications.

1.4.4 SAML Integration

In this option, the customer can use Oracle Adaptive Access Manager as an authentication service provider. Oracle Adaptive Access Manager authenticates users against LDAP or other supported authentication mechanisms, generating SAML assertions on success.

1.5 Oracle Adaptive Access Manager Architecture

Oracle Adaptive Access Manager can be installed in an n-tier deployment to allow horizontal as well as vertical scalability.

[Figure 1–1](#) shows the relationship between the Internet, the Web/Application Server that hosts OAAM Admin and OAAM Server, and the database that stores Oracle Adaptive Access Manager's data.

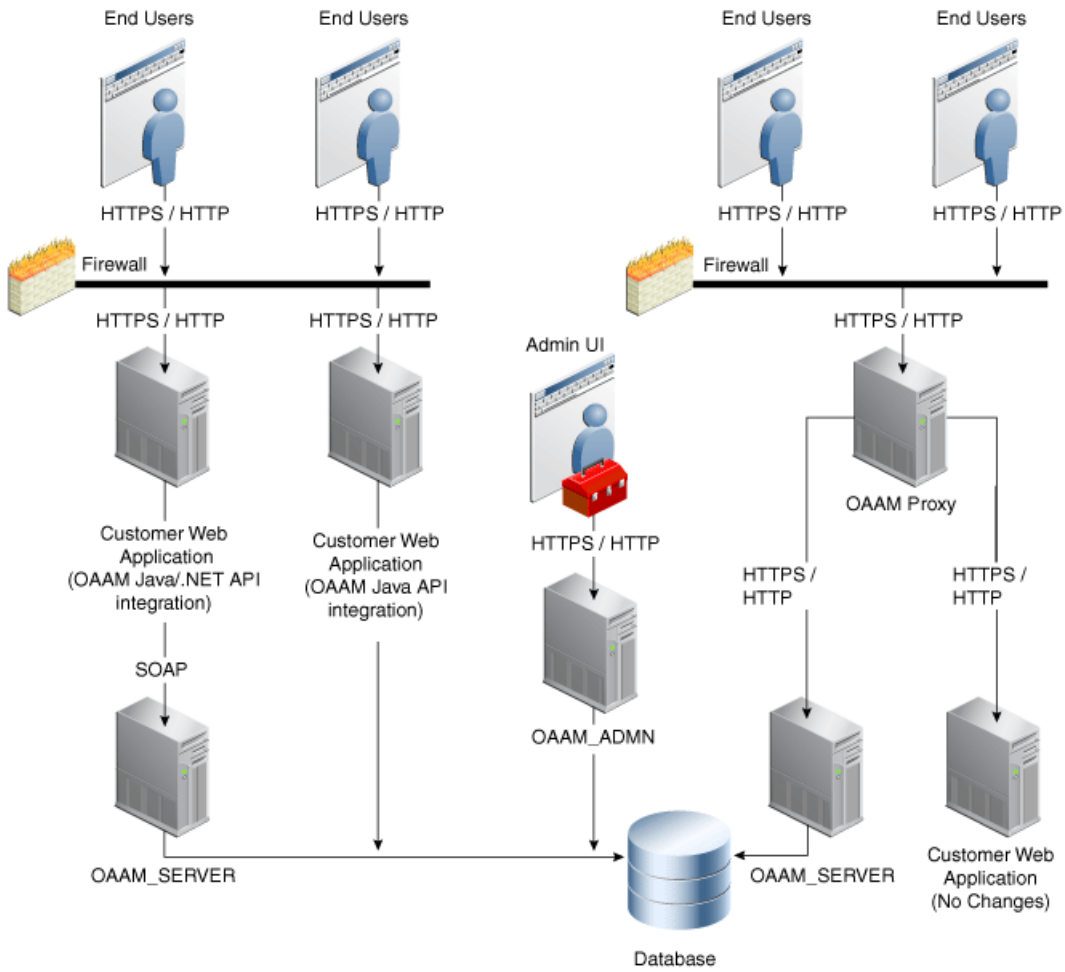
The Web server accepts requests from the browser and forwards all site traffic to the Oracle Adaptive Access Manager engine for processing. To store and retrieve configuration data, the processing engine of OAAM communicates with the database through the JDBC or JNDI driver. The Application Server is able to access and store data in the database at all times.

1.5.1 Architectural Scenario for Deployment

[Figure 1–1](#) depicts an architectural scenario for deployment.

In this scenario, Oracle Adaptive Access Manager is separated for performance and scalability, and horizontal scalability for the OAAM Admin and database.

Figure 1-1 Sample deployment scenario for performance and scalability



Setting Up the Oracle Adaptive Access Manager Environment

All tasks in this book presume that you have Oracle Adaptive Access Manager 11g 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.

2.1 Installation and Configuration

The *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* 11g 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 11g 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 Basic Environment

After installing and configuring Oracle Adaptive Access Manager, you must complete the following tasks to set up the basic 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](#)
- [Importing Challenge Questions](#)
- [Importing Base Policies](#)
- [Importing Conditions Library](#)

- [Importing Configurable Action Templates](#)
- [Importing Basic Authentication-Related Entities](#)
- [Importing IP Location Data](#)
- [Setting Properties to Enable Autolearning and Configurable Actions](#)
- [Setting the Time Zone Used for All Time Stamps in OAAM Admin](#)

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 OAAM Admin.

For information on setting up the CLI environment, see [Section 23.2, "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 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 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.

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 Fusion Middleware Control to add database credentials (username 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.

2.4.2 Pre-requisites

Pre-requisites 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 11g 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 11g, 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 11g.

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 like this:

```
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 config_secret_key.file
```

- b. In Windows

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

If the encoding command was successful, you will 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 adding 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 like this:

```
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 will 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 adding the encoded key to the Credential Store Framework.

2.4.5 Generating 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 will see the output like this:

```
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** node in the left Navigation tree.
3. Select the OAAM domain and right-click and select the menu option **Security**, and then the option **Credentials** in the submenu.
4. Find out 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 the **oaam** icon to select the map and then click the **Create Key** option.
6. In the pop-up window make sure **Select Map** is **oaam**.
7. Enter the Key Name as **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.
8. Select the **Type** as **Generic**.

9. Enter the encoded value of the symmetric key as the credential value.
10. Enter description of this in the **Description** field.
11. Click **OK** to save the secret key to the Credential Store Framework
12. Make sure you back up the alias and the secret key.

These will be 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 will become 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 left Navigation tree.
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 the **oaam** icon to select the map and then click the **Create Key** option.
6. In the pop-up window make sure **Select Map** is **oaam**.
7. Enter the **Key** as **oaam_db_key**. Make sure there are no typos and spaces.
8. Select the **Type** as **Password**.
9. Enter the database username of OAAM in the **User Name** field.
10. Enter the database password of OAAM in the **Password** field.
11. Enter the description.

2.4.8 Backing Up Secret Keys

It is important to back up the secret keys (both database-related and configuration-related). Make sure you note the secret key and the alias name.

If you delete and recreate the WebLogic 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 Importing Challenge Questions

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.

Default questions are shipped along with Oracle Adaptive Access Manager in the `oaam_kba_questions_<locale>.zip` files, which are located in the `MW_HOME/IDM_ORACLE_HOME/oaam/init/kba_questions` directory. The locale identifier `<locale>` specifies the language version.

You must load the ZIP files for the languages you want to support into Oracle Adaptive Access Manager before users can be asked to register. These questions may also be required to log in to OAAM Server.

For information on importing challenge questions, see [Section 6.5.6, "Importing Questions."](#)

2.6 Importing Base Policies

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

Base policies are shipped along with Oracle Adaptive Access Manager in the `oaam_sample_policies_for_uio_integration.zip` file, which is located in the `MW_HOME/IDM_ORACLE_HOME/oaam/init` directory.

If you want to use these policies, you must import them into your system by following these instructions:

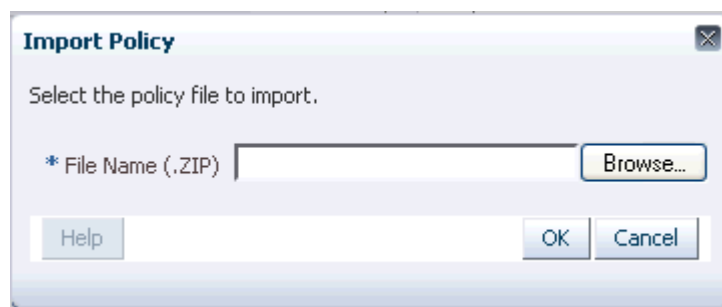
1. Create a `\tmp` folder in the drive where you have installed Weblogic if OAAM Admin is installed on the Windows platform.

For example, if the Weblogic domain is on the C drive, you would create a `c:\tmp` folder.

This folder will be used as a temporary folder for uploading large files into the OAAM Admin application.

2. In the Navigation tree, double-click **Policies**. The **Policies Search** page is displayed.
3. In the **Policies Search** page, click the **Import Policy** button. The **Import Policy** screen appears.

Figure 2–1 Import Policy



4. In the **Import Policy** dialog box, type the path and `oaam_sample_policies_for_uio_integration.zip`; or use the **Browse (...)** button to locate `oaam_sample_policies_for_uio_integration.zip`, and then select it.
5. Click **Open** and then click **OK**.

A confirmation dialog appears with the list of policies that have been successfully uploaded.

6. Click **Done** to dismiss the confirmation dialog.

The policies should be listed in the **Search Results** table of the **Policies Search** page.

2.7 Importing Conditions Library

Conditions consist of parameters that are used to evaluate datapoints collected during a checkpoint such as time, user name, authentication type, transaction data, IP, and so on.

A library of conditions used to configure rules is shipped along with Oracle Adaptive Access Manager in the `oaam_rule_conditions.zip` file, which is located in the `MW_HOME/IDM_ORACLE_HOME/oaam/rule_conditions` directory.

To use these conditions, import them into your system by following the instructions in [Section 9.24, "Importing Conditions."](#)

2.8 Importing Configurable Action Templates

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.

Configurable action templates are shipped along with Oracle Adaptive Access Manager in the `OOTB_Configurable_Actions.zip` file, which is located in the `MW_HOME/IDM_ORACLE_HOME/oaam/init` directory.

To use these templates, import them into your system by following the instructions in [Section 15.13, "Importing Action Templates."](#)

Note: If you are upgrading from Oracle Adaptive Access Manager 10.1.4.5 to Oracle Adaptive Access Manager 11g, you will 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 11g are globalized and hence the difference.

2.9 Importing Basic Authentication-Related Entities

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

Basic required entities are shipped along with Oracle Adaptive Access Manager in the `Auth_EntityDefinition.zip` file, which is located in the `MW_HOME/IDM_ORACLE_HOME/oaam/init` directory.

Before you begin using the Autolearning feature, you must import these basic entities into your system.

Import them into your system by following the instructions in [Section 16.8, "Importing Entities."](#)

2.10 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 23.4, "Importing IP Location Data."](#)

2.11 Setting Properties to Enable Autolearning and Configurable Actions

The following properties must be set to enable autolearning and configurable action features.

Autolearning

Enable the following properties so that Oracle Adaptive Access Manager collects profiling data:

- `vcrypt.tracker.autolearning.enabled` is set to true.

If this property is absent, the default is for autolearning to be enabled. If the property is present, the assigned value is used.

- `vcrypt.tracker.autolearning.use.auth.status.for.analysis` is set to true

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` is set to true

This property must be set to true for the transaction-related patterns to work. Transaction related patterns are the one that process the transaction related data for Autolearning. An example is a pattern that profiles users who are performing wire transfer operations.

Configurable Actions

To enable the configurable actions feature, set `dynamicactions.enabled` to true.

2.12 Setting the Time Zone Used for All Time Stamps in OAAM Admin

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

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

For example,

```
oaam.adf.timezone = Atlantic/Reykjavik
```

The property takes the standard values for the time zone as listed in [Section 2.12.1, "Values for the Common Timezones."](#)

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 will be formatted as per British locale formatting but the time zone will still be Pacific Time.

2.12.1 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)

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.

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:

- [Access Level to OAAM Admin](#)
- [Signing In to Oracle Adaptive Access Manager 11g](#)
- [OAAM Admin Console and Controls](#)
- [Navigation Panel](#)
- [Navigation Tree](#)
- [Policy Tree](#)
- [Management Pages](#)
- [Online Help](#)

3.1 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 3-1](#) for general descriptions of the roles.

For information on the Navigation and Policy trees, see [Section 3.5, "Navigation Tree"](#) and [Section 3.6, "Policy Tree."](#)

Table 3–1 Access Level

Oracle Adaptive Access Manager 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. 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 can access the Navigation tree and configure such items as policy set, patterns, rules, groups, and so on. They do not have access to environment properties, system snapshots, and the security dashboard, and view-only access to cases.
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. Analysts work with security investigators and CSRs to identify the policies that require adjustment and new policies that must be created.	Business analysts have read-only access the Navigation tree and cases. They do not have access to environment properties and system snapshots.
System administrator	A system administrator configures environment-level properties and transactions.	System administrators have limited access to OAAM Admin to manage the server environment. 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 11g 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*.

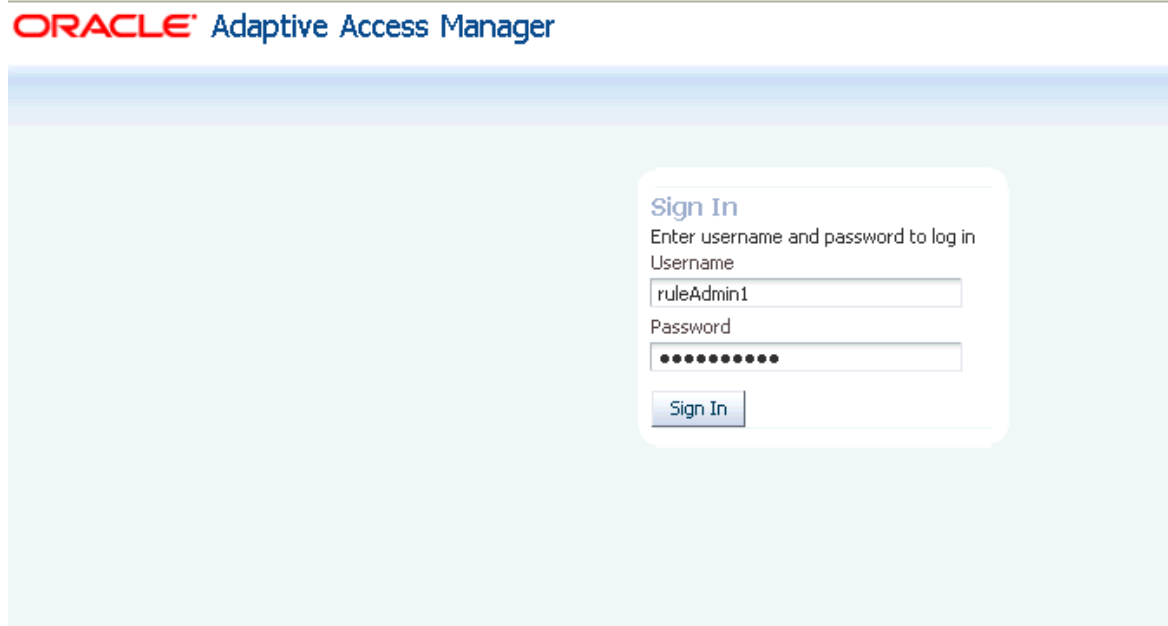
3.2 Signing In to Oracle Adaptive Access Manager 11g

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.

3.3 OAAM Admin Console and Controls

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

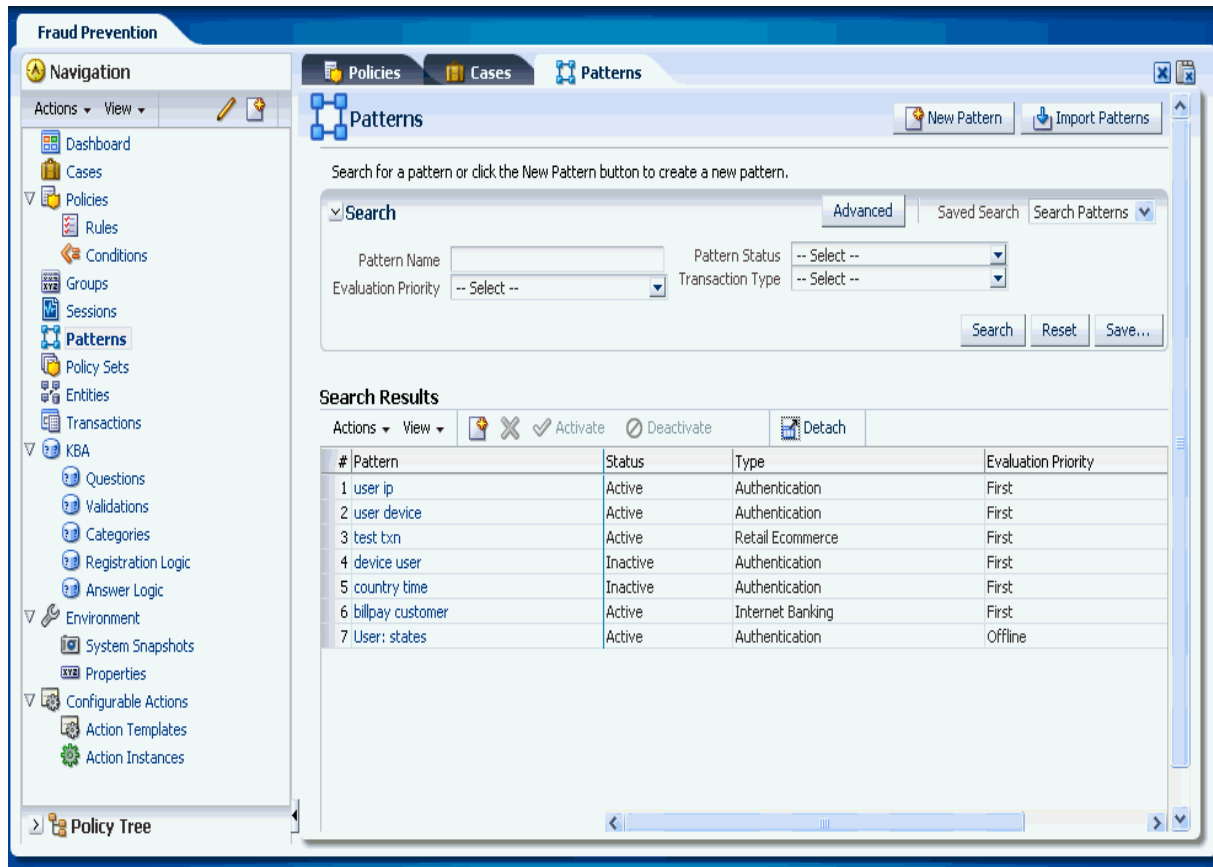
The Console is divided into the following areas: navigation panel on the left and the main, active page on the right.

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. 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](#)

3.4 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](#)

3.5 Navigation Tree

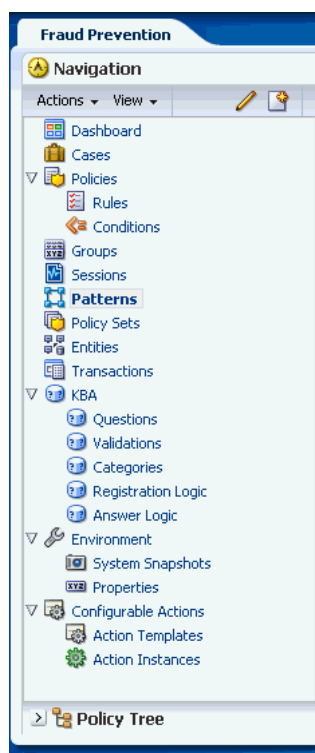
The Navigation tree, illustrated in [Figure 3–3](#), is a collapsible and expandable tree that provides quick and visible access to features of Oracle Adaptive Access Manager.

3.5.1 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 3–2 *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)
Policies	Access feature for designing policies to evaluate and handle business activities or potentially risky activities

Table 3–2 (Cont.) OAAM Features

Features	Function
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.
Environment	Access feature to manage Oracle Adaptive Access Manager environment.
Configurable Actions	Access feature to create custom actions

3.5.2 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 launches the corresponding create page of the selected node. **Create New** is available only for certain nodes where applicable. See [Table 3–3, "Create New of Selected Nodes"](#) for a list of pages launched by **Create New**.

Table 3–3 Create New of Selected Nodes

Node	Subnode	Create Screen
Dashboard		N/A
Sessions		Not available
Cases		Create Case
Policy Sets		Not available
Policies		New Policy
	Rules	Not available
	Conditions	Not available

Table 3–3 (Cont.) Create New of Selected Nodes

Node	Subnode	Create Screen
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
Environment		Not available
	Snapshots	Not available
	Properties	New Property

Open

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

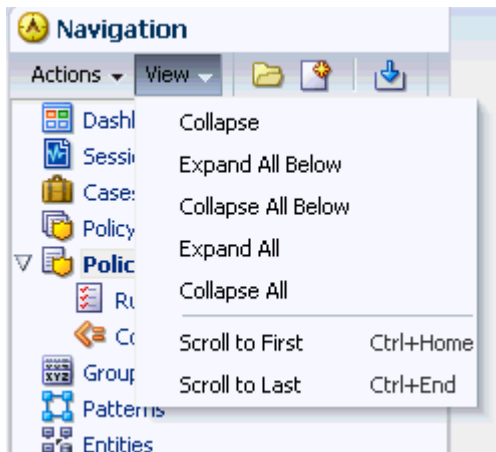
Import

Import opens the Import screen 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 3–4 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 3–5 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.

3.6 Policy Tree

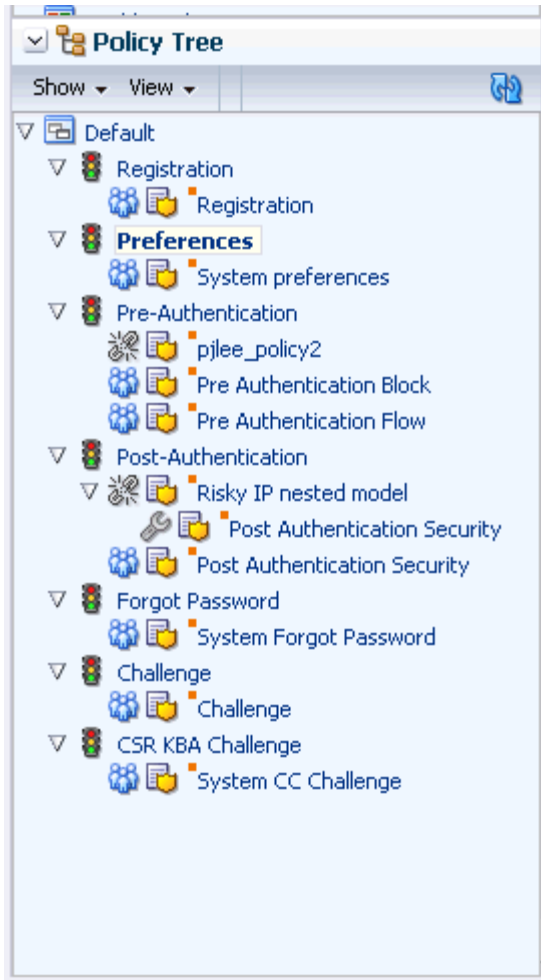
The Policy tree gives a visual representation of the policy hierarchy and the relationship between different policies, user groups, and the checkpoints.

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 3–6 provides a legend for the icons which appear on the Policy tree.

Table 3–6 Policy Tree Legend








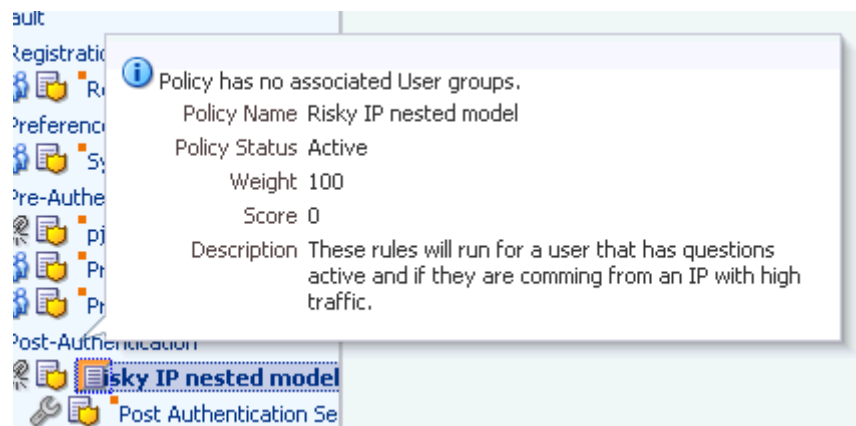
Icon	Definition	Description
	Checkpoint	The checkpoint is a decision and enforcement point when policies are call to run their rules.
	Policy	<p>The policies available in the system.</p> <p>Disabled policies are grayed out.</p> <p>Policies linked to multiple user groups are bolded and highlighted.</p> <p>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.</p> <p>To view nested policies, expand the policy node.</p>

Table 3–6 (Cont.) Policy Tree Legend

Icon	Definition	Description
	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.



3.7 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 3-7](#).

Table 3-7 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
KBA		Not available
	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
	Snapshot	Snapshots search page
	Properties	Properties search page

3.7.1 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 will 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.

3.7.1.1 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 **Create Saved Search** screen. The **Create Saved Search** screen 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.

Figure 3–8 Create Saved Search

The screenshot shows a dialog box titled "Create Saved Search". It features a text input field labeled "* Name" containing the text "myspecialsearch". Below this field are three checkboxes: "Set as Default" (checked), "Run Automatically" (checked), and "Save Results Layout" (unchecked). At the bottom of the dialog are "OK" and "Cancel" buttons.

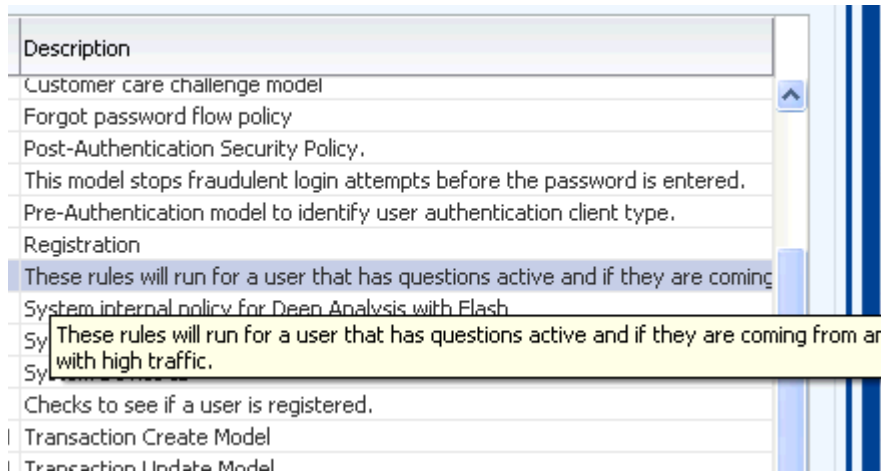
3.7.1.2 Search Results Table

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.



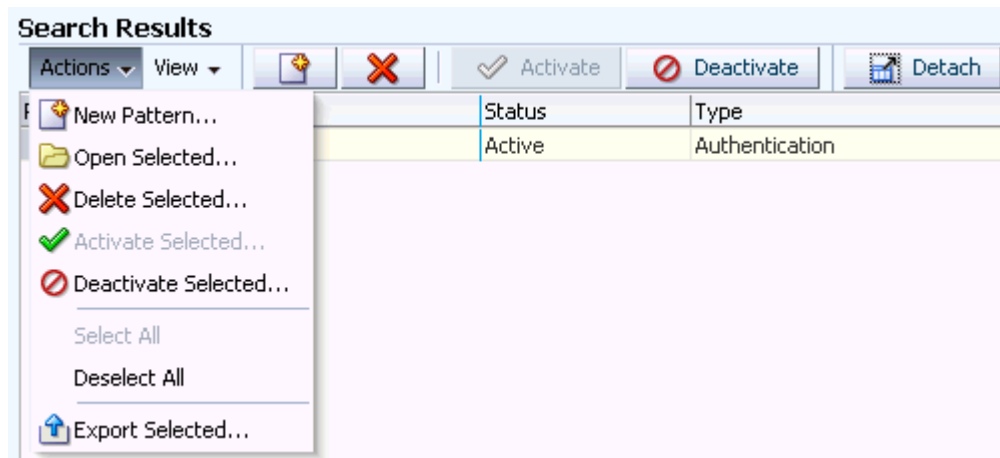
Once an item is selected in the **Search Results** table, an action can be performed on it by clicking one of the icons on the toolbar or by selecting a command from the **Actions** menu.

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

3.7.1.3 Search Results Menu and Toolbar

A menu and toolbar appears above the **Search Results** table. [Figure 3-9](#) shows the **Search Results Menu and Toolbar** from the **Patterns Search** page.







Figure 3-9 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 3-9](#) shows command buttons that may be available, depending on the selection.

Table 3–8 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.
	Activate	Activates the selected item.
	Deactivate	Deactivates the selected item.
	Detach	Detaches the Results table.

3.7.1.4 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.



3.7.1.5 Create and Import

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

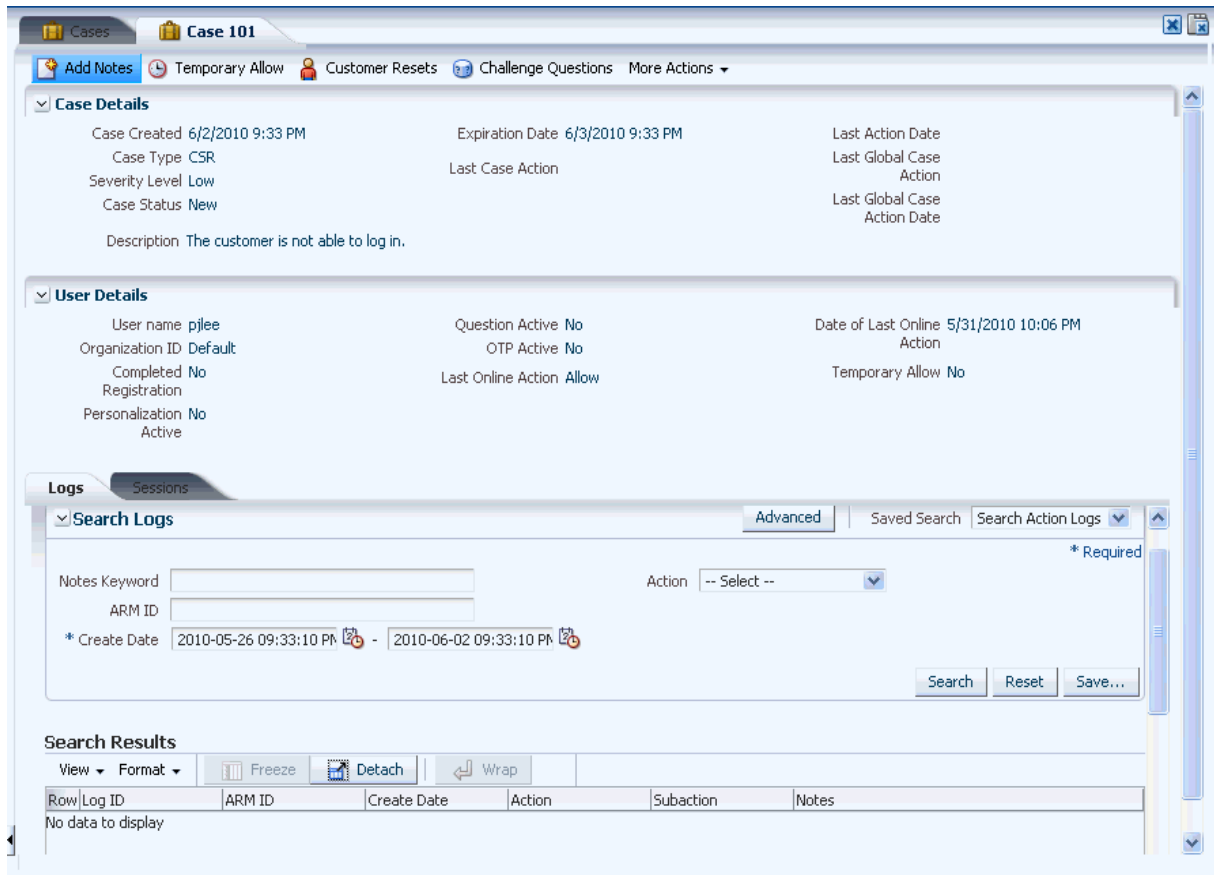


3.7.2 Detail Pages

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

A **Case Details** page is shown in [Figure 3–10](#).

Figure 3–10 Case Details



3.8 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.

3.9 Access to Search, Create, and Import

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

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.

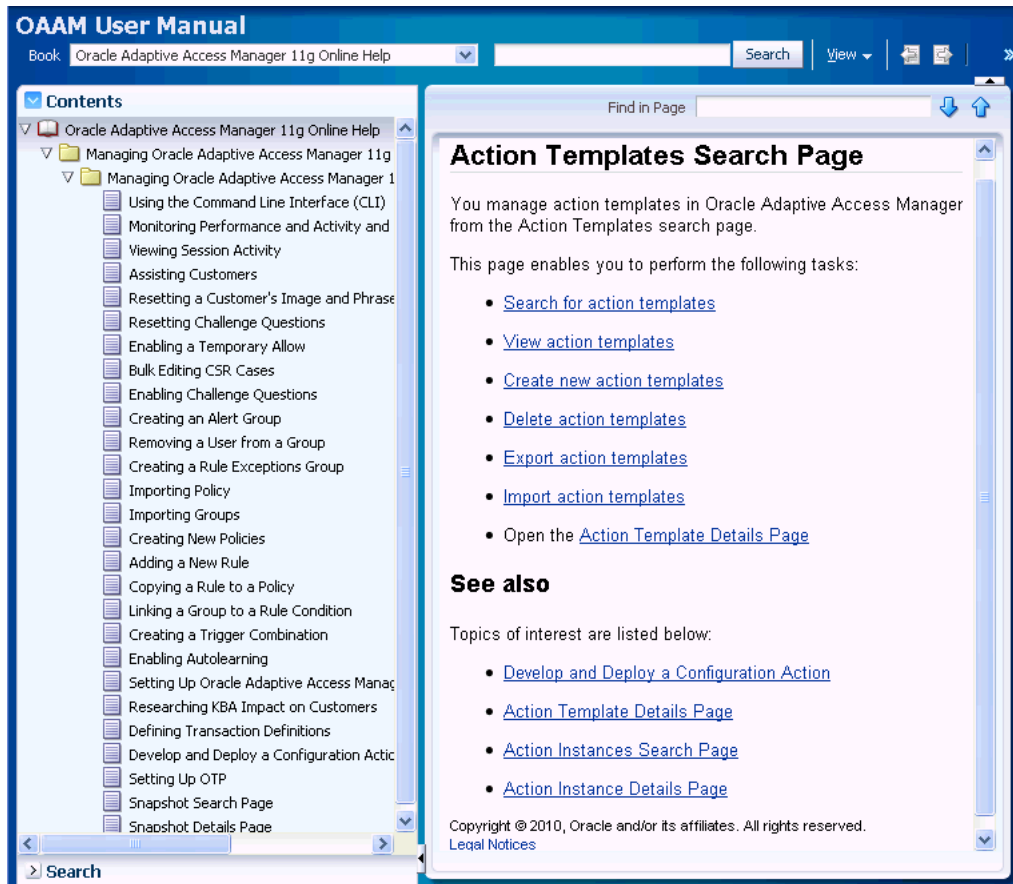
3.10 Online Help

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.



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 18, "Using the Dashboard"](#)
- [Chapter 4, "Managing and Supporting Cases"](#)

Managing and Supporting 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](#)
- [Bulk-Editing CSR Cases \(CSR Manager Only\)](#)
- [Performing Customer Resets](#)
- [Performing Challenge Question Resets](#)
- [Enabling a Temporary Allow \(CSR Manager Only\)](#)
- [Adding Notes to Cases](#)
- [Changing Severity Level of a Case](#)
- [Changing Status of a Case](#)
- [Extending Expiration \(CSR Manager Only\)](#)
- [Escalating Cases](#)
- [Configuring Expiry Behavior for CSR Cases](#)
- [Reporting](#)
- [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](#)

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

When a case is identified as a potential fraudulent activity that needs additional investigation, it is escalated. Both CSR and CSR Managers can escalate a case. An escalated case is handled and closed by a Fraud Investigator and associated with the specific user whom the case is created for. CSR and CSR Manager can view details and add notes, but cannot perform actions on the 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.

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

Locked is the status that Oracle Adaptive Access Manager sets if the user fails a challenge. 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 reopen a closed case. CSR Managers and Investigators can reopen 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 4.18, "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 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 OAAM Admin. 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 open and closed cases.	Search for CSR and escalated 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 Transactions in Sessions tab (CSRs do not have access to Session details from Queries)	View escalated case logs and notes View closed case details View Transactions in Sessions tab
Edit Case	Add notes to closed cases (view only for everything else) Perform all customer and KBA resets on a CSR case Perform KBA phone challenge on a CSR case Change status and severity on a CSR case	Reopen closed cases Add notes to CSR cases Change status and severity on a CSR case Bulk edit CSR cases Escalate 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

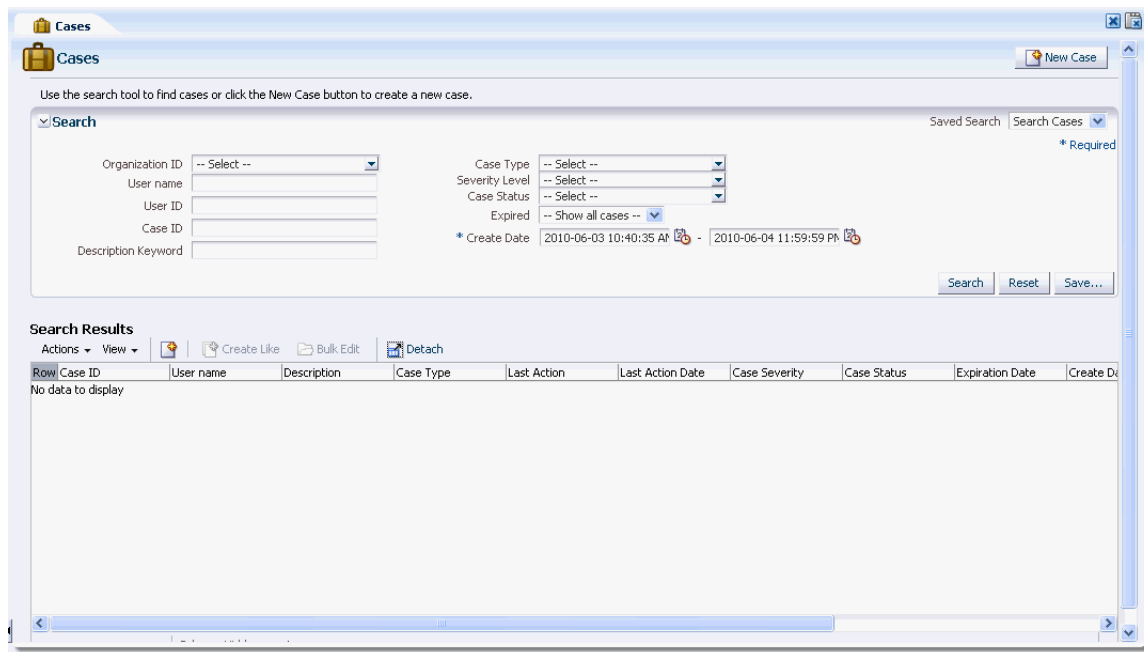
If you are a CSR, you can open only one case at a time. CSR Managers, Investigators, and Investigation Managers can open multiple case tabs.

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 login 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.
User name	To locate cases for a specific user, enter his user name or part of a user name in the Username 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.
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 filter the list by expired, select the option you want. The options available are: <ul style="list-style-type: none"> ■ Hide Expired ■ Show Only Expired
Create Date	To locate 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: <ul style="list-style-type: none"> ■ Confirmed Fraud ■ Duplicate ■ False Negative ■ False Positive ■ Issue Pending ■ Issue Resolved ■ Not Fraud <p>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.</p>

2. Click Search.

Figure 4–2 Cases Search page

The screenshot displays the 'Cases Search' page. At the top, there is a 'New Case' button. Below it, a search tool is available. The search criteria include:

- Organization ID: -- Select --
- User name: [Text Field]
- User ID: [Text Field]
- Case ID: [Text Field]
- Description Keyword: [Text Field]
- Case Type: -- Select --
- Severity Level: -- Select --
- Case Status: -- Select --
- Expired: -- Show all cases --
- * Create Date: 2010-05-26 09:23:53 PM - 2010-06-02 09:23:53 PM

Buttons for 'Search', 'Reset', and 'Save...' are present. Below the search tool is the 'Search Results' section, which includes a table of results and buttons for 'Create Like', 'Bulk Edit', and 'Detach'.

Row	Case ID	User name	Description	Case Type	Last Action	Last Action Date	Case Severity
1	101	pjee	The customer is not able to log in.	CSR			Low
2	14	nandini	The customer forgot challenge question answers.	CSR	Change Status - Penc	5/22/2010 1:10 AM	Medium
3	13	nandini	The customer forgot challenge question answers.	CSR	Change Severity - Me	5/22/2010 12:39 AM	Medium
4	12	nandini	The customer forgot challenge question answers.	CSR	Challenge Questions -	5/22/2010 12:06 AM	Medium
5	11	supriya	The customer forgot challenge question answers.	CSR			Low
6	10	nandini	The customer forgot challenge question answers.	Agent	Escalate - Escalate to	5/21/2010 11:24 PM	Medium
7	9	nandini	The customer forgot challenge question answers.	CSR	Extend Expiration Dal	5/21/2010 10:06 PM	Medium
8	8	nandini	The customer forgot challenge question answers.	CSR	Extend Expiration Dal	5/21/2010 9:48 PM	Medium
9	7	nandini	The customer forgot challenge question answers.	Agent	Escalate - Escalate to	5/21/2010 9:14 PM	Medium
10	6	supriya	The customer forgot challenge question answers.	Agent	Escalate - Escalate to	5/21/2010 9:10 PM	Medium
11	5	nandini	The customer forgot challenge question answers.	Agent	Escalate - Escalate to	5/21/2010 9:06 PM	Medium
12	4	nandini	The customer forgot challenge question answers.	CSR			Medium
13	3	nandini	The customer forgot challenge question answers.	CSR			Medium

The **Search Results** table displays a list of cases that meet the criteria you specified.

The checkbox column (1st column) is used for selecting rows. If no row is selected, the **Create Like** and **Bulk Edit** buttons are disabled.

There is a link on the case number. To view the case details, click the link.

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. Information such as **Case ID**, **Username**, **Organization ID**, **Description**, **Case Type**, **Case Status**, **Case Severity**, **Last Action Type**, **Date of Last Case Action**, and **Expiration Date** is shown for the cases listed.

4.4.3 Searching for Open and Closed Cases

- 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."](#)

- Click the case number of the case you want.

The **Case Details** page is displayed ([Figure 4–3](#)).

4.4.4 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 4–3).

4.4.5 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 username, status, severity level, and description. For information, see [Section 4.5, "Case Details Page."](#)

Figure 4–3 Case Details

The screenshot shows the 'Case Details' page for Case 101. The page is divided into several sections:

- Case Details:**
 - Case Created: 6/2/2010 9:33 PM
 - Case Type: CSR
 - Severity Level: Low
 - Case Status: New
 - Description: The customer is not able to log in.
 - Expiration Date: 6/3/2010 9:33 PM
 - Last Case Action:
 - Last Action Date:
 - Last Global Case Action:
 - Last Global Case Action Date:
- User Details:**
 - User name: pillee
 - Organization ID: Default
 - Completed Registration: No
 - Personalization Active: No
 - Question Active: No
 - OTP Active: No
 - Last Online Action: Allow
 - Date of Last Online Action: 5/31/2010 10:06 PM
 - Temporary Allow: No
- Search Logs:**
 - Advanced | Saved Search | Search Action Logs
 - Notes Keyword: [Empty]
 - ARM ID: [Empty]
 - * Create Date: 2010-05-26 09:33:10 PM - 2010-06-02 09:33:10 PM
 - Action: -- Select --
 - Buttons: Search, Reset, Save...
- Search Results:**
 - View | Format | Freeze | Detach | Wrap
 - Table Headers: Row, Log ID, ARM ID, Create Date, Action, Subaction, Notes
 - Content: No data to display

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)

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 ID 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.

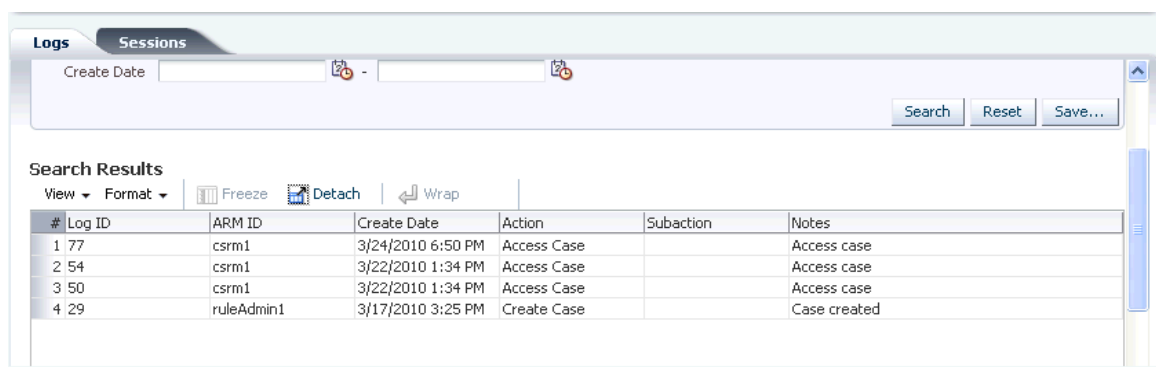
4.6 Viewing Case Activity

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 4-4 Logs Tab



#	Log ID	ARM ID	Create Date	Action	Subaction	Notes
1	77	csrm1	3/24/2010 6:50 PM	Access Case		Access case
2	54	csrm1	3/22/2010 1:34 PM	Access Case		Access case
3	50	csrm1	3/22/2010 1:34 PM	Access Case		Access case
4	29	ruleAdmin1	3/17/2010 3:25 PM	Create Case		Case created

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 4-4](#)).

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
Create 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 **Escalated** cases for Alex's username.

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 4-3](#)).

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 4–5 Sessions Tab

Session ID	Authentication Status	Login Time	Device ID	Location	Transactions	Alert Level
556	Success	7/27/2009	519	denmark, kobenha...		Low(0), Medium(1), High(0), Info(0)
531	Wrong password	7/21/2009	519	denmark, kobenha...		Low(0), Medium(1), High(0), Info(0)
530	Wrong password	7/21/2009	519	denmark, kobenha...		Low(0), Medium(1), High(0), Info(0)

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 4–5](#)).

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 ID for the session. For example, 11702.
Device ID	The device ID. 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.

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

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 by username for all cases for that user. 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 4–6 Create Case

2. Enter the **Organization ID** and **User name** or only the **User ID**.

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.

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

The **Username** is case-sensitive.

The unique **Organization ID** and **User name** combination must be available in the system.

If the username is invalid or does not use the correct uppercase and lowercase, an error message appears when you press **Create**.

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** field, or multiple descriptions from the **Description** list, or both.

You can enter any description, for example, if a customer calls and says that he or she cannot "do banking," you could create a case for the customer with the description "can't do banking."

Description is a required field. The **Create** button is disabled until a description is entered.

The **Description** field can contain alphanumeric and special characters, but it should not exceed 4000 characters.

You can select multiple descriptions from the **Description** list for the same case.

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.

5. 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.

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 4–7 Create Like

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

Description is a required field. The **Create** button is disabled until a description is entered.

You can select multiple descriptions from the **Description** list for the same case.

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.

If you are entering a description, the **Description** field can contain alphanumeric and special characters, but it should not exceed 4000 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 Bulk-Editing CSR Cases (CSR Manager Only)

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**.

The **Bulk Edit** screen is displayed.

Figure 4–8 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.

4.10 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.

4.10.1 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 will appear if you try to reset his image.

To reset a customer's image:

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 4–3](#)).
3. On the menu bar, click **Customer Resets**.

The **Customer Resets** screen is displayed.

Figure 4–9 Customer Resets

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

4.10.2 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. 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 4–3](#)).
3. On the menu bar, click **Customer Resets**.
The **Customer Resets** screen is displayed.
4. In the **User Item** list, select **Phrase**.
5. In the **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.

4.10.3 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. 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 4-3](#)).
3. On the menu bar, click **Customer Resets**.
The **Customer Resets** screen is displayed.
4. In the **User Item** list, select **Image and Phrase**.
5. In the **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.

4.10.4 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. 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 4-3](#)).
3. On the menu bar, click **Customer Resets**.
The **Customer Resets** screen is displayed.
4. In the **User Item** list, select **Unregister Devices**.
5. In the **Notes** list, select the note you want to add.
6. Edit the default notes in the **Notes** field.
7. Click **Submit**.

4.10.5 Resetting OTP Profile

When a customer's OTP profile is reset, the system deletes the contact information that is used to send the OTP.

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 will be asked to reregister OTP information at the next login.

To reset a customer's OTP profile:

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 4-3](#)).
3. On the menu bar, click **Customer Resets**.
The **Customer Resets** screen is displayed.
4. In the **User Item** list, select **Reset OTP profile**.
5. In the **Notes** list, select the note you want to add.
6. Edit the default notes in the **Notes** field.
7. Click **Submit**.

4.10.6 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. 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 4-3](#)).
3. On the menu bar, click **Customer Resets**.
The **Customer Resets** screen is displayed.
4. In the **User Item** list, select **Reset Authentication Pad**.
5. In the **Notes** list, select the note you want to add.
6. Edit the default notes in the **Notes** field.
7. Click **Submit**.

4.10.7 Unlock 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. 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 4-3](#)).
3. On the menu bar, click **Customer Resets**.
The **Customer Resets** screen is displayed.
4. In the **User Item** list, select **Unlock OTP**.
5. In the **Notes** list, select the note you want to add.

6. Edit the default notes in the Notes field.
7. Click **Submit**.

4.10.8 Resetting a Customer's Challenge Questions, Question Set, Image, and Phrase

The **Customer (All)** option resets the challenge questions, question set, image, and phrase. Afterward, inform the customer that security registration is required at the next log in to the Web site.

To reset a customer's challenge questions, question set, image, and phrase:

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 4-3](#)).
3. On the menu bar, click **Customer Resets**.
The **Customer Resets** screen is displayed.
4. In the **User Item** list, select **Customer (All)**.
5. In the **Notes** list, click the note you want to add.
6. Edit the default notes in the **Notes** field.
7. Click **Submit**.

4.11 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

4.11.1 Performing Challenge Questions Related Actions

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

1. From the **Cases Search** page, search for the case you want.
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 4-3](#)).
3. On the menu bar, select **More Actions**, and then click **Challenge Questions**.
The **Challenge Questions** screen appears.

Figure 4–10 Challenge Questions

4.11.2 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 4.11.1, "Performing Challenge Questions Related Actions."](#)
2. In the **Item** list, select **Reset Questions**.
3. In the **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 4.13, "Adding Notes to Cases"](#)) and change the status of the case if necessary ([Section 4.15, "Changing Status of a Case"](#)).

4.11.3 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 4.11.1, "Performing Challenge Questions Related Actions."](#)
2. In the **Item** list, select **Reset Question Set**.
3. In the **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 4.13, "Adding Notes to Cases"](#)) and change the status of the case if necessary ([Section 4.15, "Changing Status of a Case"](#)).

4.11.4 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 4.11.1, "Performing Challenge Questions Related Actions."](#)
2. In the **Item** list, select **Next Question**.
3. In the **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 4.13, "Adding Notes to Cases"](#)) and change the status of the case if necessary ([Section 4.15, "Changing Status of a Case"](#)).

4.11.5 Unlocking a Customer (KBA)

When you unlock a customer, he or she will be forced to register new questions and answers the next time he successfully logs in. A customer is locked when he or she fails to answer a KBA challenge more than the set threshold.

To unlock the customer:

1. Open the **Challenge Questions** screen, as described in [Section 4.11.1, "Performing Challenge Questions Related Actions."](#)
2. In the **Item** list, select **Unlock Customer**.
3. In the **Notes** list, select the note you want to add.
4. Click **Submit**.

After unlocking the user you can close the case if desired ([Section 4.15, "Changing Status of a Case"](#)).

4.11.6 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 4.11.1, "Performing Challenge Questions Related Actions."](#)
2. In the **Item** list, select **Ask Question**.
3. In the **Notes** list, select **User Challenged**.

If you select **User Challenged**, the **Notes** field will contain 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. Enter the customer's answer in the **Answer** field.
7. Click **Submit**.

4.12 Enabling a Temporary Allow (CSR Manager Only)

To enable a temporary allow:

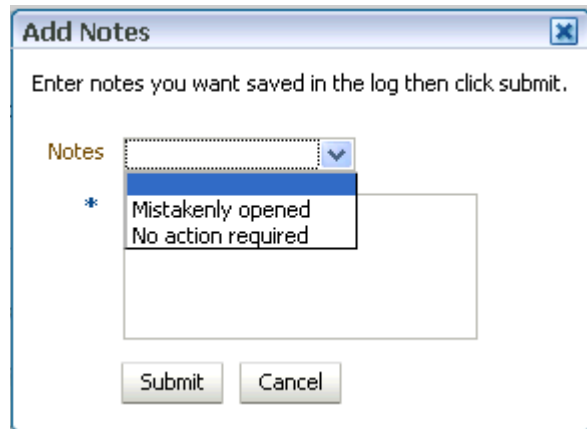
1. Search for the case from the **Cases Search** page.
For information, see [Section 4.4.1, "Searching for Cases."](#)
2. Click the case number of the case you want.
The **Case Details** page appears ([Figure 4-3](#)).
3. Click **Temporary Allow** on the menu bar.
4. In the **Allow** list, select the 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 **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 will be on his trip for three months and should receive an exception for that time.
7. Click **Submit**.

4.13 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 4-3](#)).
3. Click **Add Notes** on the menu bar.
The **Add Notes** screen appears.

Figure 4–11 Add Notes

4. 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.

4.14 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 4–3](#)).
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 **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**.

4.15 Changing Status of a Case

Status refers to the current state of a case, to whether it is 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 4-3](#)).
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**.

4.15.1 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 4-3](#)).
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 **Notes** list or enter a new note.
7. Click **Submit**.

A confirmation dialog is displayed.

8. Click **OK**.

4.15.2 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 4-3](#)).
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 **Notes** list or enter a new note.
8. Click **Submit**.
A confirmation dialog is displayed.
9. Click **OK**.

4.15.3 Reopening Closed Cases (CSR Manager Only)

To reopen 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 4-3](#)).
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**.

4.16 Extending Expiration (CSR Manager Only)

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 4-3](#)).
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 **Notes** list, click the note you want you want to add.
7. Click **Submit**.

4.17 Escalating Cases

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 4-3](#)).
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. In the **Notes** list, select the note that describes the case.
7. Click **Submit**.

4.18 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 22, "Using the Properties Editor."](#)

4.19 Reporting

For information on how CSRs use the reporting functionality of Oracle Adaptive Access Manager, see [Chapter 19, "Configuring BI Publisher Reports."](#)

4.20 Use Cases

The following sections provide scenarios of how Oracle Adaptive Access Manager's investigation tools are used.

4.20.1 Use Case: Customer Session Search and Case Creation

Carl is Dollar Bank CSR.

One of the users "Tim" who is blocked, calls Carl and asks him to create a case for his blocked status.

1. Carl searches sessions and creates a case.
 - 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 then finds it expired, so he reopens it.
4. Carl also escalates the case. After escalation he will no longer see 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 case saying she will work on it.

4.20.2 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 SSN. His Login 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 Login ID and verify his home address and last four digits of his SSN.
4. Search open cases by user.

Search for Henry's open cases by entering xxxx into the **Login 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 username, xxxx, in the **Login 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 **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.

4.20.3 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 **Login 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 **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.

4.20.4 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 **Create 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.

4.20.5 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 **Create Date** column for the four cases in the **Search Results** table.

- All are more than two days old. (View **Create 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.

4.21 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.

Using Session Details

The **Session Details** page records information about sessions and enables easy access to key information required by the investigators, analyst, and customer care personnel.

It contains a forensic record of the session, including transactions and checkpoints that ran. Each checkpoint contains lists of triggered actions and alerts as well as the policies and rules. General session data points are also listed on this page, such as user, device, location, and others.

A **Session Details** page displays an overview of the events that transpired during a particular session for fraud analysis.

This chapter includes the following topics:

- [Searching for a Session](#)
- [Viewing Session Details](#)
- [Uses Cases](#)
- [Comparison Between 10g and 11g Session Details](#)

5.1 Getting Started

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.

5.2 Searching for a Session

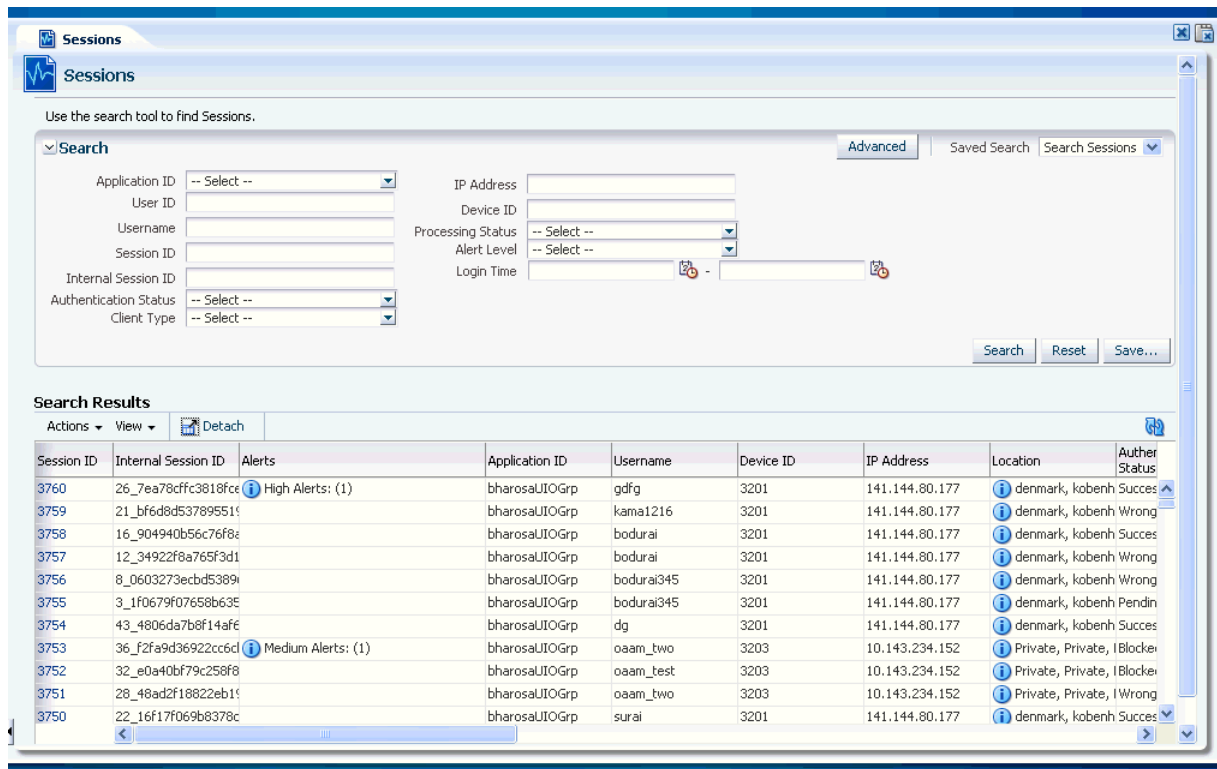
To search for sessions:

1. Log in to OAAM Admin as an investigator.
2. In the Navigation tree, double-click **Sessions**. The **Sessions Search** page is displayed.

Alternatively, you can 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 5–1 Sessions Search Page



3. Search for the session by the details you are interested in.

The filters are:

- Organization ID
- User ID
- Username
- Session ID
- Authentication Status
- IP Address
- Device ID
- Alert Level
- Login Time

For example, you can 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**).

5.3 Navigating to the Session Details Page

To go to the **Session Details** page:

1. In the **Search Results** table, click the **Session ID** of the session you are interested in. The **Session Details** page for that session is displayed.

All of the actions are captured in one session. You can view the actions the user performed during the session time.

After you know the details and whereabouts of the user, you would want to know the different checkpoints you ran.

2. In the **Session Details** page, click the **Checkpoint** tab to see the **Device Identification**, **Pre-Authentication**, and **Post-Authentication** details.

5.4 Viewing Session Details

The **Session Details** page consolidates information needed for fraud analysis.

5.4.1 The Panels

The **Session ID** is displayed on the tab label. The tab label shows the session ID to identify the session you are working with.

The **Session Details** page contains several panels. Except for the **Session Details** and **Login Details** panels, all other panels are displayed in the order of execution. All panels are collapsible. The main panels like checkpoints and transactions have multiple subpanels. Panels are not displayed if information is not available. For example, if there are no configurable actions for that session, the configuration actions panel is not displayed.

5.4.2 Session Details Panel

The top most panel, the **Session Details** panel, contains all the general information related to that session, such as the request ID, session ID, device score, Organization ID, and location.

5.4.3 Login Details Panel

The next panel after the **Session Details** panel is the **Login Details** panel.

The **Login** panel shows all the related information regarding the login (transaction). It shows the status, authentication status, IP address from which the user logged in, username, user ID, cookie information, autolearning processing status, and the login time.

5.4.4 Checkpoint Panels

The next panel is for checkpoint #1. Other checkpoint panels follow.

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.

Alerts

Alerts that were triggered during the session for the checkpoint are displayed. High-level alerts are displayed in bold red.

Actions

All actions are displayed in the **Actions** panel with 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.)

Policies

A list of policies in that checkpoint are displayed in the **Policies** panel. The scoring engine information is not available for rules. Only the policy scoring engine is displayed. 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.

5.4.5 Transactions Panel

The transactions panel displays a list of transactions that were performed in this session along with their corresponding transaction ID, transaction data, and entity information. You can also view the actual transaction data and the entity attribute values used in the transactions. For example, you can view the transaction amount in the bill pay transaction. Information such as this is helpful for the forensics.

5.4.6 Policy Explorer

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

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

You have the 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.

5.5 Uses Cases

This section describes example use cases for the Session Details page.

5.5.1 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**.

5.5.2 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 screen 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 on 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 **Login Details** panel, the **Authentication Status** shows **Blocked**.
3. View the final outcomes of each checkpoint.
 - a. Click the **Checkpoint** panel.
 - b. Expand the checkpoints.
 - c. View the post-authentication checkpoints.
 - d. Expand the post-authentication policies.
 - e. Click the policy of interest to show details about the policy.

- f. View the rules that are triggered.
- g. 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 username 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.

5.6 Comparison Between 10g and 11g Session Details

In 11g, the **Session Details** page has been redesigned.

Starting from 11g, key information regarding a session is contained on one screen rather than on different screens.

For example, in 10g, if you were on the **Session Details** page and wanted to know if a manual override existed in a policy, you would have to navigate away to another page.

The 11g **Session Details** page is better for forensics. For example, if you were analyzing a particular session, you would want all the details in one place. In 10g, values that were passed into a session are not available on the page. If a user were blocked during a transaction, and you were looking at the session, you would know the particular rule that was triggered and that the user was blocked when he was performing a transaction. However, you would not have the information about the amount that was passed in, the account number that was used in the transaction, and so on.

For example, in 10g, you would not know if there was a configurable action that added the user to a blacklisted group. Although you would know if Autolearning was turned on and what the processing status was, details would not be available about the pattern or the buckets that were updated.

Part III

Managing KBA and OTP

This part of the book provides information on managing Knowledge-Base Authentication (KBA) and OTP.

It contains the following chapters:

- [Chapter 6, "Managing Knowledge-Based Authentication"](#)
- [Chapter 7, "Enabling Challenge Questions"](#)
- [Chapter 8, "Setting Up OTP Anywhere"](#)

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](#)
- [Configuring the Answer Logic](#)
- [Setting Up a KBA Failure Counter](#)
- [Use Cases](#)
- [KBA Guidelines and Recommended Requirements](#)

6.1 Introduction and Concepts

This section describes knowledge based authentication (KBA) key concepts.

6.1.1 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 username 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.

6.1.2 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.

6.1.3 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.

6.1.4 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.

6.1.5 Challenge Questions

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. These are configured through properties.

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

6.1.6 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.

6.1.7 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. The drop-down with questions is called a "menu."

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 will be applied to the answers

For information on setting Registration Logic, see [Section 6.8, "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 will register: 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.

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 will 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, 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."

6.1.8 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 level of Answer 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 OAAM Server. 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.

6.1.9 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.

6.1.10 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.

A success for an online or a phone challenge automatically resets all counters to zero. For the next challenge, the next question is displayed.

6.1.11 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.

6.1.11.1 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.

6.1.11.2 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.

6.1.11.3 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.

6.1.11.4 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.

6.1.11.5 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 6.1.10, "Failure Counters."](#) High level flows for the Ask Question action is presented in [Chapter 4, "Managing and Supporting Cases."](#) The matrix in [Section 6.1.10, "Failure Counters"](#) contains detailed examples for individual flows.

6.1.12 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.

	New customers	user with question in question set	users with question registered
Disable 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. If the user is re-registering or changing user preference, the disabled question is replaced with another question from the same category.

	New customers	user with question in question set	users with question registered
Disable 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. 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.

6.1.13 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.

6.2 Setting Up KBA Overview

This section outlines the steps to manage the library, registration and answer processing of the challenge questions.

6.2.1 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 2.5, "Importing Challenge Questions."](#)

6.2.2 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 6.7.2, "Creating a New Category."](#)
- Create Questions
 - Create questions that can be applicable to the users accessing your application.
 - For information, see [Section 6.5.3, "Creating a New Question"](#) and [Section 6.14.2, "Guidelines for Designing Challenge Questions."](#)
- Apply Validations
 - Apply validations to the questions.
 - For information, see [Section 6.6.2, "Adding a New Validation."](#)

6.2.3 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 6.8, "Configuring the Registration Logic."](#)

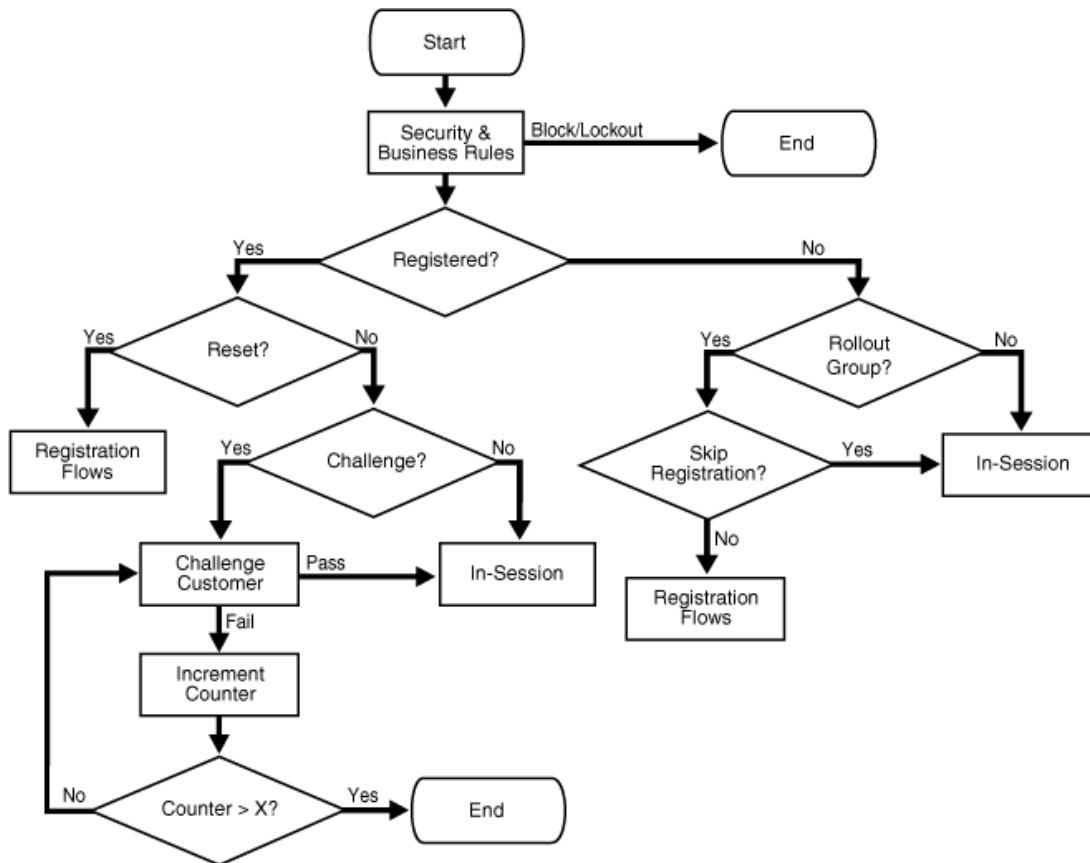
- Set up the Answer Logic - The Answer Logic settings can be configured for the exactness required for challenge question answers and for answering threshold/tolerance, such as the level of fat fingering, typos, abbreviations, and so on.

For information, see [Section 6.9, "Configuring the Answer Logic."](#)

6.2.4 User Flow

The following diagram illustrates the user experience with the KBA framework implemented.

Figure 6-1 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 OAAM Server page.
2. On the first sign in page, enter <user name> in the **Username** 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 screen 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 OAAM server 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 **Username** 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.

6.3 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 7, "Enabling Challenge Questions."](#)

Task	[]
Ensure that base policies are installed	[]
Link the appropriate policies to the user group that you want KBA to be enabled for.	[]
Ensure that KBA properties are set	[]
Upload the challenge questions using OAAM Admin	[]
Import and enable policies for your security and business needs	[]
Change the rules within the registration and challenge policies with appropriate actions	[]

6.3.1 Ensuring that Universal Installation Option Base Policies are Installed

If you are using pre-packaged policies, ensure that the base policies are installed. If you are not using pre-packaged policies, use this chapter as a guideline for enabling challenge questions.

Oracle Adaptive Access Manager is shipped with default policies packaged into two ZIP files.

The default policies are available in `oaam_init` in the `MW_HOME/IDM_ORACLE_HOME/oaam/init` directory.

If you want to use these policies, import them into your system by following the instructions in [Section 9.16.2, "Importing a Policy."](#)

6.3.2 Ensuring that KBA Properties/Default Properties are Set

Ensure that the `bharosa.kba.active` property is set to `true`. See [Chapter 22, "Using the Properties Editor"](#) for information on modifying properties.

6.3.3 Uploading Challenge Questions

The challenge questions must be loaded in Oracle Adaptive Access Manager before the users can be asked to register.

For information on importing challenge questions, see [Section 2.5, "Importing Challenge Questions."](#)

6.3.4 Importing and Enabling Policies

Import KBA security policies that pertain to your business and security needs and link them to a user group to which you want KBA to be enabled.

For information on importing policies, see [Chapter 9, "Managing Policies, Rules, and Conditions."](#)

6.3.5 Configuring Rules for Registration and Challenge Policies

Change the rules within the policies for your needs.

6.4 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, "Access to 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.

6.5 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](#)

- [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](#)
- [Deactivating Questions](#)

6.5.1 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.

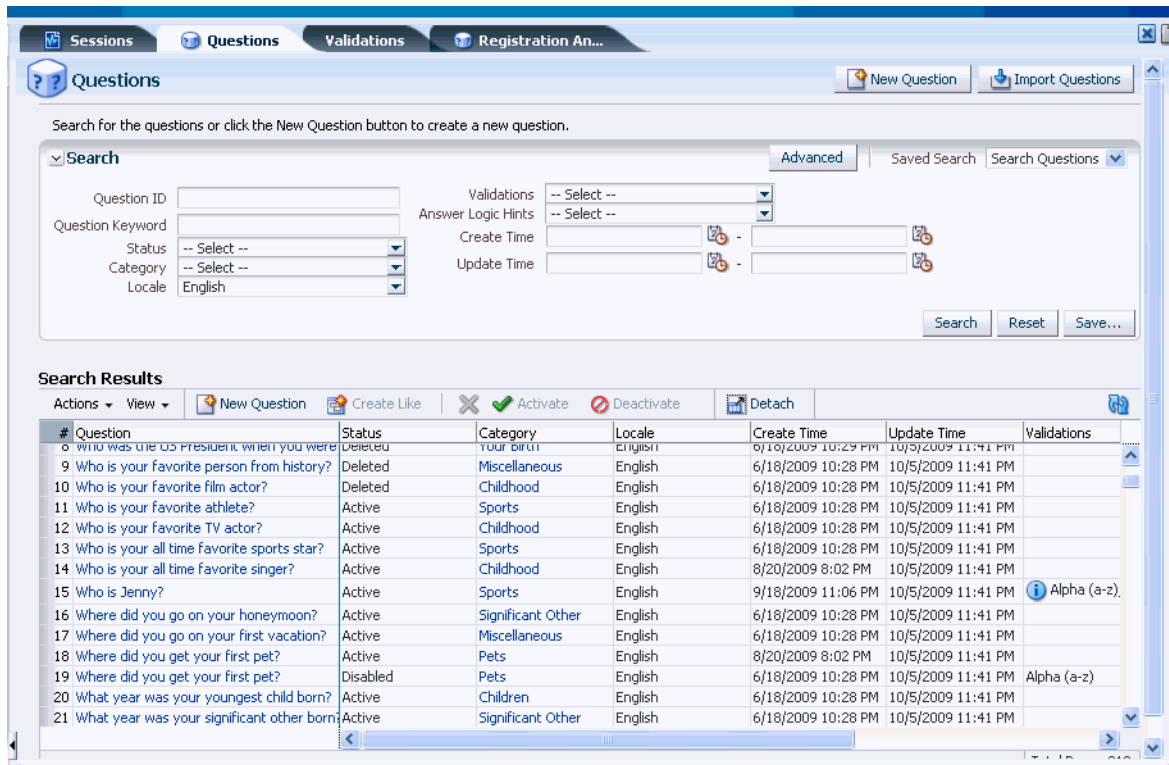
When the **Questions Search** page first appears, the **Search Results** table is displayed with default filter values.

To search for a question:

1. Navigate to the **Questions Search** page, as described in [Section 6.4, "Accessing Configurations in KBA Administration."](#)

An example **Questions Search** page is shown in [Figure 6-2](#).

Figure 6-2 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.

- Specify criteria in the Search Filter to locate the questions and click **Search**.

The search filter criteria are described in [Table 6–1](#).

If you want to reset the search parameters to the default setting, use the **Reset** button.

Table 6–1 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.
Create Time	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**, **Create Time**, **Status**, **Question**, and **Category**.

In the **Search Results** table, click the question link to view more details. The **Question Details** page appears.

[Table 6–2, "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 6–2 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.

6.5.2 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 6.4, "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.

6.5.3 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, "Access to 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. Type the new question in the **Question** field.
The question names must be unique across categories.
4. 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.

5. In the **Locale** list, select the language you want.

By default, the **Locale** menu displays English and 26 other default locale languages.

6. 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 6.1.9, "Validations."](#)

7. 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.

8. Click **Apply**. A confirmation dialog appears telling you that the question was created successfully.
9. 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.

6.5.4 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 6.4, "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** screen appears where you can enter details to create a new question.

The **Create Like** screen 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.

6.5.5 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 6.4, "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.

6.5.6 Importing Questions

To import questions:

1. Navigate to the **Questions Search** page, as described in [Section 6.4, "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** screen, 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**.

6.5.7 Exporting Questions

Multiple questions can be selected and exported.

To export questions:

1. Navigate to the **Questions Search** page, as described in [Section 6.4, "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** screen, click the **Export** button.
The selected questions are exported.

6.5.8 Deleting a Question

To delete a question, follow these instructions.

1. Navigate to the **Questions Search** page, as described in [Section 6.4, "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.

Deleted questions are not available for new registrations but the user currently registered for these questions can continue to use them.

6.5.9 Disabling a Question

To disable a question

1. Navigate to the **Questions Search** page, as described in [Section 6.4, "Accessing Configurations in KBA Administration."](#)
2. In the **Questions Search** page, search for the question you want to disable.
3. Click the hyperlinked question you want to disable.

The **Question Details** page appears.

4. In the **Status** field, select **Disable** and click **Apply**.

The selected questions are disabled.

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.

6.5.10 Activating Questions

To activate questions:

1. Navigate to the **Questions Search** page, as described in [Section 6.4, "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.

6.5.11 Deactivating Questions

To deactivate questions:

1. Navigate to the **Questions Search** page, as described in [Section 6.4, "Accessing Configurations in KBA Administration."](#)
2. In the **Questions Search** page, search for the questions you want to deactivate.
3. Select the rows corresponding to the questions you want to deactivate.
4. Press the **Deactivate** button or select **DeActivate** from the **Actions** menu.

The selected questions are deactivated.

The following scenarios occur when a question is deactivated:

- The deactivated question is not used to generate a new question set.
- At re-registration or reset, the deactivated question is replaced with another question from the same category for those users who had the deactivated question in their question set.
- The deactivated question remains active for users who have registered the question. If the user is re-registering or changing user preference, the deactivated question is replaced with another question from the same category.

6.6 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 6.1.9, "Validations."](#)

6.6.1 Using the Validations Page

The **Validations** page enables you to perform the following functions:

- [Adding a New Validation](#)
- [Editing an Existing Validation](#)
- [Exporting Validations](#)
- [Deleting Validations](#)

Navigate to the **Validations** page, as described in [Section 6.4, "Accessing Configurations in KBA Administration."](#)

An example **Validations** page is shown in [Figure 6–3](#).

Figure 6–3 *Validations Page*

Row	Validation Name	Validation Type	Last Updated
1	Alpha (a-z)	Regular Expression	6/28/2010 12:34 PM
2	Alphanumeric (a-z, 0-9)	Regular Expression	6/28/2010 12:34 PM
3	Alphanumeric and limited special characters (A-Z, a-z, 0-9 and !@#\$%^&()-=_+`~[])	Regular Expression	6/28/2010 12:34 PM
4	Four digit year (YYYY)	Date	6/28/2010 12:34 PM
5	Max Len	Maximum Length	6/30/2010 3:09 PM
6	Maximum Length (30 Characters)	Maximum Length	6/28/2010 12:34 PM
7	Maximum Length (50 Characters)	Maximum Length	6/28/2010 12:34 PM

By default, validations are sorted on **Validation Name**, but you can sort validations on **Updated**.

[Table 6–3, "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 6–3 *Validation Action menu commands*

Command	Description
Add	Adds a new validation.
Import	Imports validations
Export	Exports validations
Delete	Deletes validations

6.6.2 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 6.4, "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 screen 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 6–4 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 "MMddy" 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

Table 6–4 (Cont.) Validation Parameters

Validation Type	Label for Fields	Description for Validation Parameter	Example for note
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
Repeated Character	Enter Number of Repeating Characters	Allowed number of repeated characters in the answer. If the answer entered by the user contains repeated characters more than the configured value, the validation fails and the user gets a configured error message.	Example: 3
Repeated Answers	Enter Number of Repeating Answers	Allowed number of repeated answers. For example parameter value can be '1' for unique answer validation. If the answer entered by the user is repeated more than configured number of times, the validation fails and the user gets a configured error message.	Example: 1
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.

6.6.3 Editing an Existing Validation

To edit an existing validation

1. Navigate to the **Validations** page, as described in [Section 6.4, "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 6–4, "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.

6.6.4 Exporting Validations

To export validations:

1. Navigate to the **Validations** page, as described in [Section 6.4, "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** screen appears, select **Save File**, and then **Save**.

The file is exported and saved as a ZIP file.

6.6.5 Deleting Validations

To delete validations:

1. Navigate to the **Validations** page, as described in [Section 6.4, "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.

6.7 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](#)

6.7.1 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.

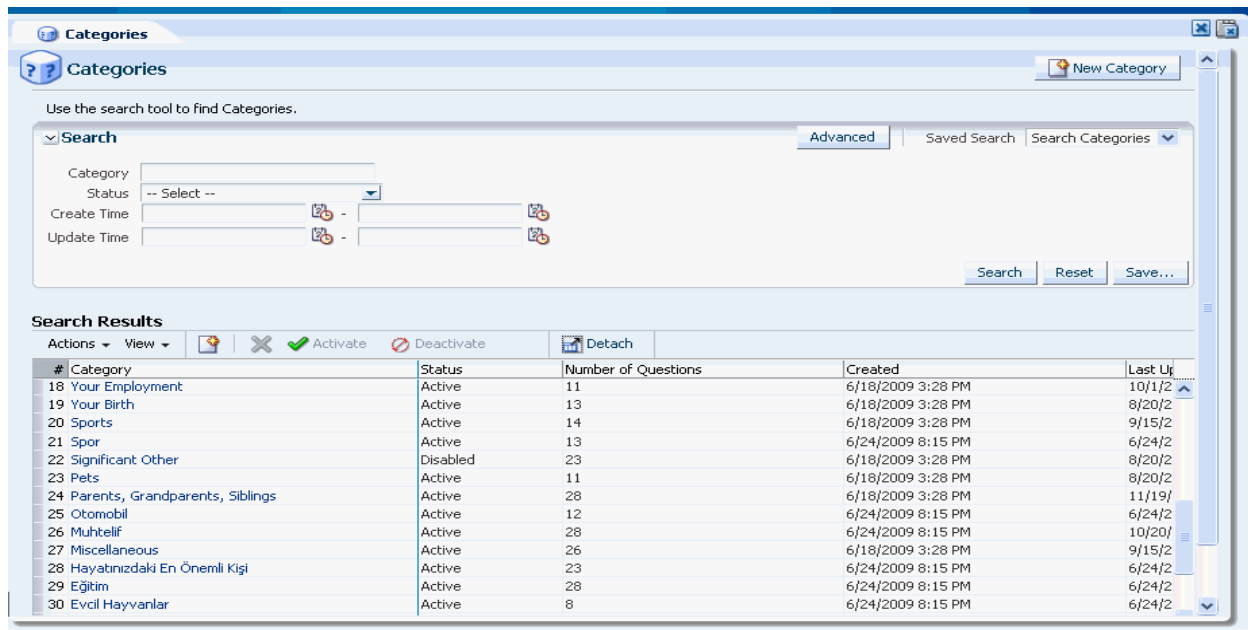
When the **Categories Search** page first appears, the **Search Results** table displays results from the default search values.

To search for a category:

1. Navigate to the **Categories Search** page, as described in [Section 6.4, "Accessing Configurations in KBA Administration."](#)

An example **Categories Search** page is shown in [Figure 6-4](#).

Figure 6–4 Categories Search page



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.

- Specify criteria in the Search Filter to locate the specific question category and click **Search**.

The search filter criteria are described in [Table 6–1](#).

If you want to reset the search parameters to the default setting, use the **Reset** button.

Table 6–5 Question Search Criteria

Field	Description
Category	The category name. For example: education, pets, sports and so on.
Status	The status of the category.
Create Time	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.

6.7.2 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

- Navigate to the **Categories Search** page, as described in [Section 6.4, "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, "Access to 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.

6.7.3 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 6.4, "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.

6.7.4 Deleting Categories

To delete a category, follow these instructions.

1. Navigate to the **Categories Search** page, as described in [Section 6.4, "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.

6.7.5 Activating Categories

To activate categories:

1. Navigate to the **Categories Search** page, as described in [Section 6.4, "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.

6.7.6 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 6.4, "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.

6.8 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."

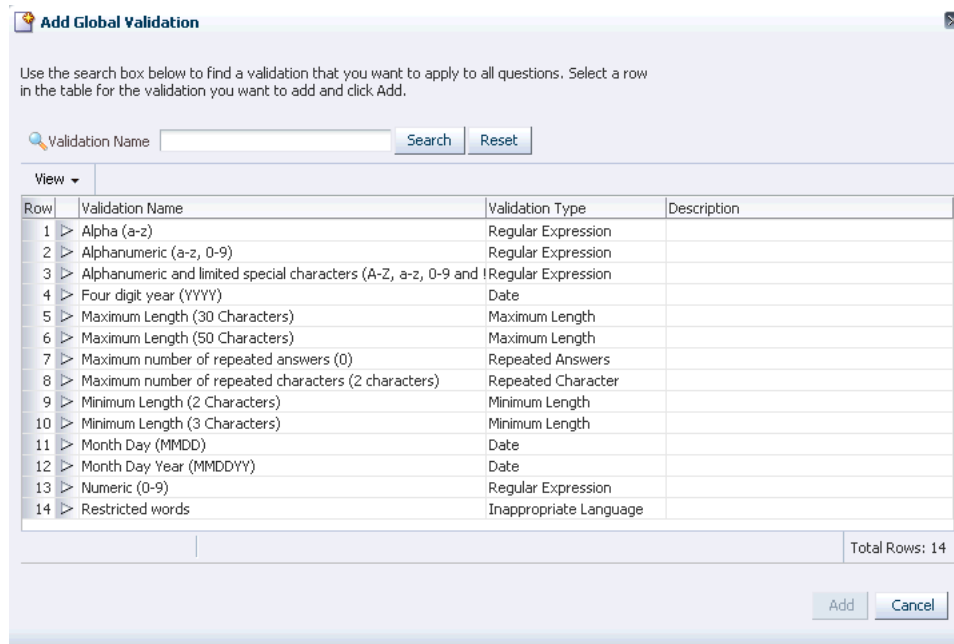
4. Click **OK**.

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** screen appears.

Figure 6–5 Add Global Validation



3. In the **Add Global Validation** screen, 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 screen 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.

6.9 Configuring the Answer Logic

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

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.

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.

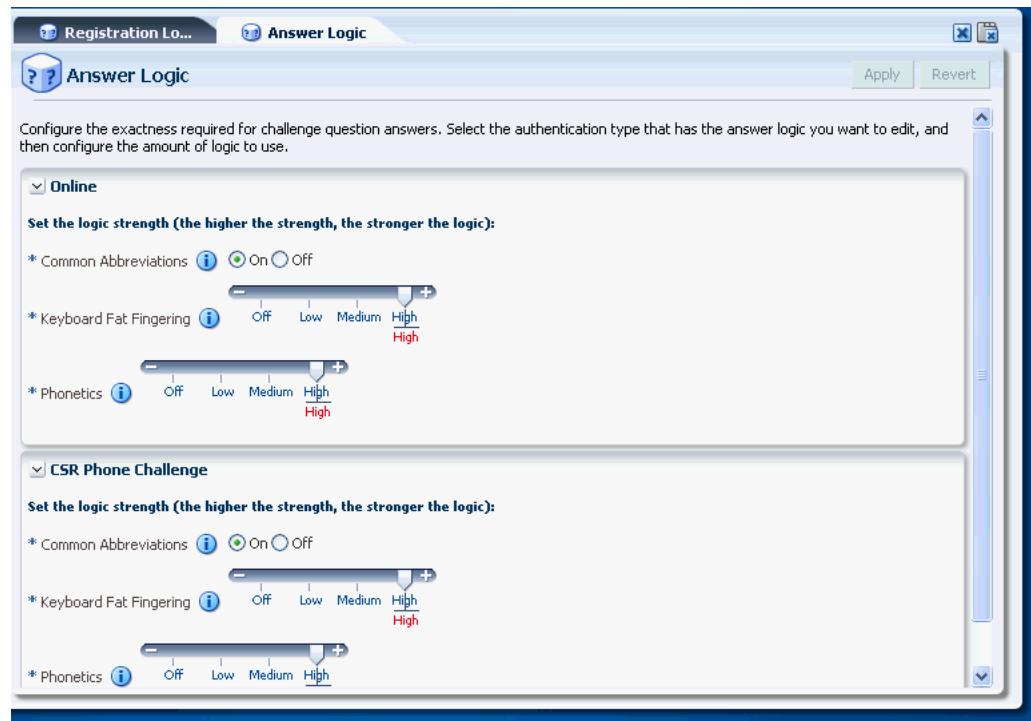
Answer Logic (fuzzy logic) algorithms can be configured on the Answer Logic page. The algorithms are divided into three categories: Common Abbreviations, Fat Fingering (accidentally pressing the nearest neighbor on the keyboard), and Phonetics.

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 6.11, "Customizing Abbreviations and Equivalences for Locales."](#)

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 6–6 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 6.9.3, "Level of Answer Logic."](#)
3. Click **OK**.

6.9.1 About Answer Logic

The Answer Logic algorithms can be enabled or disabled and the intensity or strength of some algorithms can also be configured.

The following Answer Logic algorithms are available for both the online challenge and phone challenge processes:

Abbreviations

This algorithm handles common abbreviations, common nicknames, common acronyms, and date format.

Phonetics

This algorithm handles Answers that "sound like" the registered answer, regional spelling differences, and common misspellings

Keyboard fat fingering

This algorithm handles Answers with typos due to the proximity of keys on a standard keyboard.

6.9.2 Answer Logic Algorithms Examples

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.

6.9.2.1 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 6.10, "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

6.9.2.2 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

6.9.2.3 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

6.9.3 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.

6.9.3.1 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

6.9.3.2 Fat Fingering

For fat fingering:

- Return values: range 0 to 100
- Levels: **OFF**, **LOW** (90+), **MEDIUM** (75+), **HIGH** (60+)
- Logic
 - If the string lengths don't match, score is 0
 - If a position does not have the expected character or its neighbor, score is 0
 - Else compute the number of positions that have the neighboring characters.
 - $Score = (StringLength - NeighborPositionCount) * 100 / StringLength$

6.9.3.3 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

6.9.3.4 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.

6.10 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. Using the Properties Editor, change the property, `bharosa.authenticator.AbbreviationFileName`, to point to the complete path to `custom_auth_abbreviation_config.properties`.

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 22, "Using the Properties Editor."](#)

4. Configure the Answer Logic by following the instructions in [Section 6.9, "Configuring the 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`.

6.11 Customizing Abbreviations and Equivalences for Locales

Translated files are shipped for different locales. 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`.

If you want to localize for one locale (for example, for Japanese only) you can create one file and set the value of property `bharosa.authenticator.AbbreviationFileName` to that file's absolute path.

If you want to customize for multiple locales you need to perform the following steps:

1. Create the files specific to those locales with the same prefix.

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. Set the property `bharosa.authenticator.AbbreviationFileName` to `/mydrive/IDM_ORACLE_HOME/oaam/conf/Abbreviations.properties`.

Note that the locale prefix is absent in the value of the property.

Oracle Adaptive Access Manager uses the locale specific suffixes to the base file name and calculates the file name for that locale at runtime. You only have to specify the base name of the file, independent of locale, as the property value, and Oracle Adaptive Access Manager calculates the locale specific value automatically at runtime based on that property value.

6.12 Setting Up a KBA Failure Counter

To set up a KBA failure counter, create a rule in a security policy. The rule must have the condition, "User: Challenge Maximum Failures Condition."

The rule verifies if the user failed to answer question challenges for a specified number of times.

Note: A success for a challenge automatically resets the KBA failure counters to 0.

For information on conditions, see [Appendix B, "Conditions Reference."](#)

6.13 Use Cases

This section describes example use cases for KBA.

6.13.1 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** screen, 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.

6.13.2 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** screen, 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**.

6.13.3 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**, etc.) 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 a 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 6.1.10, "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.

6.14 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.

6.14.1 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 for numeral answers will be accepted during KBA registration. This would be a problem if there are questions available to users that would normally have alphanumeric answers.

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 will not be presented with the disabled question.

6.14.2 Guidelines for Designing Challenge Questions

Guidelines for designing challenge questions are listed below:

- No confidential data used in question.
- Answers are difficult to guess.
- Answers cannot be obtained from public sources.
- Questions that are applicable to general public.
- Answers are memorable/personally significant.
- Questions where answers can change over time are avoided.
- Questions cannot pertain to religion, politics, taboo subjects, and so on.

6.14.3 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.

6.14.4 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.

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](#)
- [Ensuring that Base Policies are Installed](#)
- [Ensuring KBA Properties/Default Properties are Set](#)
- [Uploading Challenge Questions](#)
- [Importing and Enabling Policies](#)
- [Configuring Rules for Policies](#)
- [Configuring the Challenge Question Answer Validation](#)
- [Configuring the Answer Logic](#)

7.1 What is KBA?

Knowledge-based authentication (KBA) is a form of secondary authentication where the user answers personal questions to confirm identity. The user is prompted for information by using challenge questions and must provide previously registered answers during authentication. Questions can vary, and each response is encrypted at the point of entry to accurately and securely confirm identity and prevent fraud.

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.

7.2 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.

- In the first phase, the user is not registered and there is little change to the user experience.
- In the second phase, the user can choose to register.
- In the third phase, 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 three phases. The first two phases generally last between one and three months each depending on user population size and composition.

7.2.1 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.

7.2.2 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.

7.2.3 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.

7.3 Checklist for Enabling Challenge Questions

The following chart presents a checklist for enabling challenge questions.

Task	[]
Ensure UIO base policies are installed	[]
Link the appropriate policies to the user group that you want KBA to be enabled for.	[]
Ensure KBA properties are set	[]
Upload the challenge questions using OAAM Admin	[]
Import and enable policies for your security and business needs	[]
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	[]

7.4 Ensuring that Base Policies are Installed

If you are using pre-packaged policies, ensure that the base policies are installed. If you are not using pre-packaged policies, use this chapter as a guideline for enabling challenge questions.

Oracle Adaptive Access Manager is shipped with default policies packaged into two ZIP files.

The default policies are available in `oaam_init` in the `MW_HOME/IDM_ORACLE_HOME/oaam/init` directory.

If you want to use these policies, import them into your system by following the instructions in [Section 9.16.2, "Importing a Policy."](#)

7.5 Ensuring KBA Properties/Default Properties are Set

Ensure the `bharosa.kba.active` property is set to true.

7.6 Uploading Challenge Questions

The challenge questions must be created in OAAM Admin before the users can be asked to register. The Oracle Adaptive Access Manager package contains the challenge questions, in 27 languages, in ZIP files. Import questions for appropriate locales for your deployment.

For information on importing Challenge Questions, see [Section 2.5, "Importing Challenge Questions."](#)

7.7 Importing and Enabling Policies

Import KBA security policies that pertain to your business and security needs and 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.

7.8 Configuring Rules for Policies

Change the rules within the policies for your needs.

7.9 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 6.6, "Setting Up Validations for Answer Registration."](#)

7.10 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 6.9, "Configuring the Answer Logic."](#)

Setting Up OTP Anywhere

OTP Anywhere creates universal delivery options for auto-generated one-time-passwords used for secondary, risk-based user challenges to add sophisticated security to basic authentication flows.

OTP is a form of out-of-band authentication that is used as secondary credentials. It is generated at pre-configured checkpoints based on policies configured.

This chapter focuses on the setting up Oracle Adaptive Access Manager to use a configured delivery method to authenticate users.

8.1 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.

8.1.1 Out-of-Band OTP Delivery

Oracle Adaptive Access Manager 11g contains one time password authentication capabilities that support the delivery of a random server-generated OTP through any of the following out-of-band channels:

- email
- SMS
- voice messaging
- instant messaging

The user is OTP-challenged to enter the single-use PIN or password code he receives into a Web interface. This form of authentication is used as a secondary credential in addition to the static username and password.

8.1.2 One Time Password (OTP)

One Time Password (OTP) is a random single use authentication credential. The OTP may be either numeric or alphanumeric and any length and the randomization algorithm is pluggable.

The following are major benefits of using out-of-band OTP:

- The one time password is delivered to the valid user through one of the configured channels. These can include SMS, IM, email or voice.
- The user does not require any proprietary hardware or client software of any kind.

8.1.3 Registration

Registration is the enrollment process, the opening of a new account, or other event where information is obtained from the user.

During registration, the user is asked to select supported OTP delivery channels.

When OTP-challenged, the single-use PIN or password is delivered to the user through the delivery channel he selected.

8.1.4 OTP Challenge

An OTP challenge is when the user is asked to provide the OTP as a form of authentication for high risk situations based upon configured policies.

Oracle Adaptive Access Manager, depending on its configuration for OTP, sends a time-constrained single-use PIN or password to the user when further authentication is required.

The user is OTP-challenged to enter the single-use PIN or password code he receives in to a Web interface.

The user must enter the correct OTP in to the Web interface to proceed with the operation.

8.1.5 KBA vs. OTP

Oracle Adaptive Access Manager deployments may choose to use both KBA and OTP Anywhere or each separately or no challenge mechanisms at all. If both KBA and OTP Anywhere are being used in a deployment, the security team may choose to use KBA for challenges in lower risk situations and OTP Anywhere for higher risk situations.

For example, a user logging in from a new IP in a city he often logs in from is relatively low risk on its own so a KBA challenge would be 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 Anywhere enabled, the priority is configurable through properties.

For information on KBA and OTP Anywhere priority, see [Section 8.5, "Enabling OTP Challenge."](#)

8.1.6 OTP Failure Counters

An OTP failure occurs when the user supplies an incorrect answer during an OTP-challenge and the failure counter is incremented. When a correct PIN or password is provided by the user, the failure counter is reset to 0 and the user is allowed to proceed with the operation.

When the failure counter reaches the threshold value, the user is "OTP Locked."

The maximum number for OTP challenges is configurable.

OTP failures are counted across sessions.

If the user is OTP-locked, he can call the Customer Service Representative to become unlocked.

8.1.7 OTP Resets

A customer service representative (CSR) can reset a customer's OTP profile or unlock a customer when necessary.

8.1.7.1 Reset OTP Profile

The CSR resets a user's OTP profile. The system deletes the contact information that is used to send the OTP. The customer must register OTP information at the log in.

8.1.7.2 Unlock a Customer

The CSR unlocks the user who calls because he has been OTP-locked out of the system. Unlocking the customer resets the customer's OTP failure counter.

8.2 User Flow

Example use cases that follow illustrates the user experience when the OTP framework is configured.

Use Case 1: New Registration Example

This example illustrates the user registration experience.

1. The user logs in to a protected application for the first time after Oracle Adaptive Access Manager is deployed.
2. The user selects his virtual device, and personalization image and phase.
3. The user sets up KBA challenge questions.
4. The user selects one or more of the following OTP Anywhere delivery channels:
 - cell phone
 - email address
 - home phone number
 - Instant Message ID

The delivery channel used is configured by an administrator for all users in a deployment.

Use Case: User Login Example

This section illustrates an example of the user login experience when a high risk rule is triggered, and OTP Anywhere is used in the deployment.

1. A registered user logs in to a protected application.
2. If the situation is high enough risk, the user is asked to enter an OTP sent to them in another channel/band.
3. The user will enter the OTP in the web interface to authenticate himself.

8.3 Setting Up OTP Anywhere

To set up OTP Anywhere, you must perform the following tasks:

1. [Enabling OTP Profile Registration and Preference Setting](#)
2. [Setting Up the Contact Input Elements for OTP Registration Page](#)
3. [Configuring the OTP Challenge Types](#)

4. [Configuring OTP Delivery](#)

For information on customizing Oracle Adaptive Access Manager, see the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

8.3.1 Enabling OTP Profile Registration and Preference Setting

To enable OTP profile registration and preference setting:

1. In the Navigation tree, double-click **Properties** under the **Environment** node. The **Properties Search** page is displayed.
2. Search for the following properties and set them to true.

If the properties do not exist, create them.

- `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.

OTP Challenge types must be enabled before any pages are displayed.

8.3.2 Setting Up the Contact Input Elements for OTP Registration Page

If user information registration or user preferences is set to true, configure the input information for the OTP registration or preferences page. The `bharosa.uio.default.userinfo.inputs.enum` property values are shown in [Table 8-1](#).

Table 8-1 *OTP Properties for Contact Input*

Property	Description
<code>inputname</code>	Name used for the input field in the HTML form
<code>inputtype</code>	Set for text or password input
<code>maxlength</code>	Maximum length of user input
<code>required</code>	Set if the field is required on the registration page
<code>order</code>	The order displayed in the user interface

The following is an example of an enum defining mobile device registration on the OTP registration page of an authenticator:

```
bharosa.uio.default.userinfo.inputs.enum.mobile=0
bharosa.uio.default.userinfo.inputs.enum.mobile.name=Mobile Phone
bharosa.uio.default.userinfo.inputs.enum.mobile.description=Mobile Phone
bharosa.uio.default.userinfo.inputs.enum.mobile.inputname=cellnumber
bharosa.uio.default.userinfo.inputs.enum.mobile.inputtype=text
bharosa.uio.default.userinfo.inputs.enum.mobile.maxlength=15
bharosa.uio.default.userinfo.inputs.enum.mobile.required=true
bharosa.uio.default.userinfo.inputs.enum.mobile.order=1
bharosa.uio.default.userinfo.inputs.enum.mobile.enabled=true
```

The following is an example of an enum for adding a second mobile device to register:

```
bharosa.uio.default.userinfo.inputs.enum.mobile2=2
```

```

bharosa.uio.default.userinfo.inputs.enum.mobile2.name=Mobile Phone 2
bharosa.uio.default.userinfo.inputs.enum.mobile2.description=Mobile Phone 2
bharosa.uio.default.userinfo.inputs.enum.mobile2.inputname=mobile2
bharosa.uio.default.userinfo.inputs.enum.mobile2.inputtype=text
bharosa.uio.default.userinfo.inputs.enum.mobile2.maxlength=10
bharosa.uio.default.userinfo.inputs.enum.mobile2.required=true
bharosa.uio.default.userinfo.inputs.enum.mobile2.order=2
bharosa.uio.default.userinfo.inputs.enum.mobile2.enabled=true
bharosa.uio.default.userinfo.inputs.enum.mobile2.regex=\\D?(\\d{3})\\D?\\D?(\\d{3})
)\\D?(\\d{4})
bharosa.uio.default.userinfo.inputs.enum.mobile2.errorCode=otp.invalid.mobile
bharosa.uio.default.userinfo.inputs.enum.mobile2.managerClass=com.bharosa.uio.manager.user.DefaultContactInfoManager

```

The following is an example of an enum defining email registration on the OTP registration page of an authenticator:

```

bharosa.uio.default.userinfo.inputs.enum.email=1
bharosa.uio.default.userinfo.inputs.enum.email.name=Email Address
bharosa.uio.default.userinfo.inputs.enum.email.description=Email Address
bharosa.uio.default.userinfo.inputs.enum.email.inputname=email
bharosa.uio.default.userinfo.inputs.enum.email.inputtype=text
bharosa.uio.default.userinfo.inputs.enum.email.maxlength=40
bharosa.uio.default.userinfo.inputs.enum.email.required=true
bharosa.uio.default.userinfo.inputs.enum.email.order=2
bharosa.uio.default.userinfo.inputs.enum.email.enabled=true
bharosa.uio.default.userinfo.inputs.enum.email.regex=.[a-zA-Z_
]+?\\.[a-zA-Z]{2,3}
bharosa.uio.default.userinfo.inputs.enum.email.errorCode=otp.invalid.email
bharosa.uio.default.userinfo.inputs.enum.email.managerClass=com.bharosa.uio.manager.user.DefaultContactInfoManager

```

The following is an example of an enum for adding a second email to register:

```

bharosa.uio.default.userinfo.inputs.enum.email2=2
bharosa.uio.default.userinfo.inputs.enum.email2.name=Email Address 2
bharosa.uio.default.userinfo.inputs.enum.email2.description=Email Address 2
bharosa.uio.default.userinfo.inputs.enum.email2.inputname=email2
bharosa.uio.default.userinfo.inputs.enum.email2.inputtype=text
bharosa.uio.default.userinfo.inputs.enum.email2.maxlength=40
bharosa.uio.default.userinfo.inputs.enum.email2.required=true
bharosa.uio.default.userinfo.inputs.enum.email2.order=2
bharosa.uio.default.userinfo.inputs.enum.email2.enabled=true
bharosa.uio.default.userinfo.inputs.enum.email2.regex=.[a-zA-Z_
]+?\\.[a-zA-Z]{2,3}
bharosa.uio.default.userinfo.inputs.enum.email2.errorCode=otp.invalid.email
bharosa.uio.default.userinfo.inputs.enum.email2.managerClass=com.bharosa.uio.manager.user.DefaultContactInfoManager

```

8.3.3 Configuring the OTP Challenge Types

Configure the `bharosa.uio.default.challenge.type.enum` property to edit out-of-the-box OTP challenge types or add a new challenge type.

Table 8–2 Challenge type Properties

Property	Description
available	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.

Table 8–2 (Cont.) Challenge type Properties

Property	Description
processor	java class for handling challenges of this type. The challenge mechanism is customizable through Java classes. See the <i>Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager</i> for information.
requiredInfo	comma separated list of inputs from registration input enum

The following is an example of an enum defining email challenge for OTP:

```
bharosa.uio.default.challenge.type.enum.ChallengeEmail = 1
bharosa.uio.default.challenge.type.enum.ChallengeEmail.name = Email Challenge
bharosa.uio.default.challenge.type.enum.ChallengeEmail.description = Email
Challenge
bharosa.uio.default.challenge.type.enum.ChallengeEmail.processor =
com.bharosa.uio.processor.challenge.EmailChallengeProcessor
bharosa.uio.default.challenge.type.enum.ChallengeEmail.requiredInfo = mobile
bharosa.uio.default.challenge.type.enum.ChallengeEmail.available = true
bharosa.uio.default.challenge.type.enum.ChallengeEmail.enabled = true
```

The following is an example of an enum defining SMS challenge for OTP:

```
bharosa.uio.default.challenge.type.enum.ChallengeSMS = 2
bharosa.uio.default.challenge.type.enum.ChallengeSMS.name = SMS Challenge
bharosa.uio.default.challenge.type.enum.ChallengeSMS.description = SMS Challenge
bharosa.uio.default.challenge.type.enum.ChallengeSMS.processor =
com.bharosa.uio.processor.challenge.SmsChallengeProcessor
bharosa.uio.default.challenge.type.enum.ChallengeSMS.requiredInfo = mobile
bharosa.uio.default.challenge.type.enum.ChallengeSMS.available = true
bharosa.uio.default.challenge.type.enum.ChallengeSMS.enabled = true
```

8.3.4 Configuring OTP Delivery

The delivery channel used is configured by an administrator for all users in a deployment.

8.4 Configuring OTP Presentation

8.4.1 Adding an OTP Device

By default, challenge devices are configured through rules. The rules are under the Authentication Pad checkpoint and determine the type of device to use based on the purpose of the device (ChallengeEmail, ChallengeSMS, ChallengeQuestion, and so on).

Alternatively, if you want to configure challenge devices using properties, you can bypass the Authentication Pad checkpoint by setting `bharosa.uio.default.use.authentipad.checkpoint` to `false`. Then, perform the following instructions:

Edit the challenge type properties (ChallengeEmail, ChallengeSMS) so that the desired device is displayed for challenging the user.

For the example in [Table 8–3](#), PinPad has been configured as the SMS and Email authenticator.

```
bharosa.uio.default.ChallengeSMS.authenticator.device=DevicePinPad
bharosa.uio.default.ChallengeEmail.authenticator.device=DevicePinPad
```

Other device choices are listed in [Table 8–3](#).

Table 8–3 Challenge 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 login to the application.

8.4.2 Changing an OTP Device

To change the OTP Device used for challenges, change the OTP challenge type for the rule's result action.

If properties are used, change the device for the
`bharosa.uio.default.<ChallengeType>.authenticator.device=<Device>`

8.5 Enabling OTP Challenge

To enable OTP challenges:

1. In the Navigation tree, double-click **Properties**. The **Properties Search** page is displayed.
2. Search for the `bharosa.uio.default.challenge.type.enum.<challengeType>.available` property and set it to true for the OTP challenge you want.
3. If you want challenge questions enabled as well, ensure that `bharosa.uio.default.challenge.type.enum.ChallengeQuestion.available` is set to true.
4. Configure a new policy with the OTP challenge type as the result action.

In default policies, if OTP is enabled, OTP challenges occurs after a user is KBA Challenge blocked.

High risk user are KBA Challenged. If the user fails the KBA challenge, the user will be presented with the appropriate virtual authentication device and receive the OTP through the proper channel.

8.6 Setting Up 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 using the User: Check OTP failures condition.

Note: A success for an OTP challenge automatically resets the OTP failure counters to 0.

8.7 OTP Case Management

Steps for using case management actions for OTP are described in the following subsections.

8.7.1 Resetting OTP Profile

This Reset Profile option resets the OTP profile for the user.

1. From the **Cases Search** page.
For information, see [Chapter 4, "Managing and Supporting Cases."](#)
2. Click the case number of the case you want.
The **Case Details** page appears.
3. On the menu bar, click **Customer Resets**.
The **Customer Resets** screen appears.

Figure 8–1 Customer Reset

4. In the **Item to Select** list, select **Reset Profile**.
5. In the **Notes** list, click the note you want to add.
6. If you selected **Other** from the **Notes** list, enter a note describing why you are taking the action.
7. Click **Submit**.

8.7.2 Unlocking User

This action resets the OTP failure counter for the user.

An "OTP lock" occurs when a user's failure counter across sessions is greater than the threshold value specified.

As a CSR, you can unlock a user if the lock out occurred through OTP failures. To do this:

1. Search for the case from **Cases Search** page.
For information, see [Chapter 4, "Managing and Supporting Cases."](#)
2. Click the case number of the case you want.
The **Case Details** page appears.
3. On the menu bar, click **Customer Resets**.
The **Customer Resets** screen appears.
4. In the **Item to Select** list, select **Unlock Customer**.
5. In the **Notes** list, click the note you want to add.
6. If you selected **Other** from the **Notes** list, enter a note describing why you are taking the action.
7. Click **Submit**.

An OTP unlock resets the OTP failure count to 0.

Note: An "Unlock OTP" action does not affect KBA functionality and vice versa.

8.7.3 OTP Case Details

The **Case Details** page provides the following OTP-specific information:

1. In the Navigation tree, double-click **Cases**.
The **Cases Search** page is displayed.
2. Create a case for a user who has a registered OTP profile.
3. From the **Case Details**, click **Customer Resets** and select **Reset OTP Profile**. Enter notes and click **Submit**.
OTP Profile is reset. **Last Case Action** and **Last Case Action** date in **Case Details** page display the Reset OTP Profile action and date.

8.8 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.

Part IV

Managing Policy Configuration

This part contains information about managing policy configurations in Oracle Adaptive Access Manager 11g.

It contains the following chapters:

- [Chapter 9, "Managing Policies, Rules, and Conditions"](#)
- [Chapter 10, "Managing Groups"](#)
- [Chapter 11, "Managing the Policy Set"](#)
- [Chapter 12, "Using the Scoring Engine"](#)
- [Chapter 13, "Managing System Snapshots"](#)

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.

9.1 Introduction and Concepts

This section introduces you to the concept of policies and rules and how they are used in Oracle Adaptive Access Manager.

9.1.1 Policies

A policy is a collection of rules that are run in a single checkpoint. The policy is designed to evaluate and handle business activities or potentially risky activities that you may run across in the day-to-day operation of your business. For example, a business activity may be a user making a \$15,000 deposit, and a potentially risky activity may be a user making a wire transfer of more than \$10,000. The outcome of policy evaluation is a score, actions, and alerts. Policy outcomes are used to enforce business requirements. For information on rules, see [Section 9.1.2, "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 9.1.4, "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.

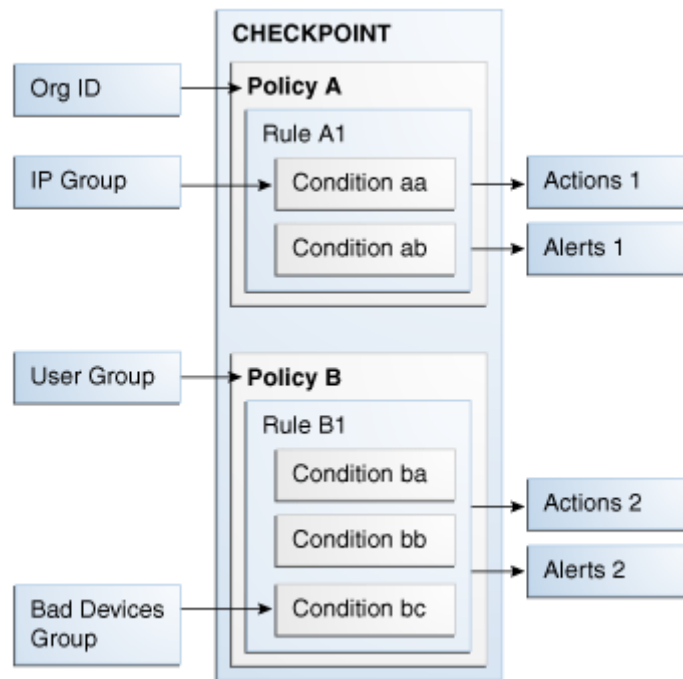
The score is based on the scoring policy selected. If you do not want a score as the outcome, you can change the outcome to be an action group and alert group by using trigger combinations. An action group is also executed based on the score. For information about trigger combinations, see [Section 9.1.10, "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

Figure 9–1 illustrates the policy structure.

Figure 9–1 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.

9.1.2 Rules

A rule is a collection of conditions. When all pre-conditions of the rule are met and all conditions evaluate to true, the rule evaluates to true. Then, the rule is assigned the user-configured score, which is further evaluated by the policy. The rule can also generate specified alerts and trigger associated actions.

9.1.3 Conditions

Conditions are configurable evaluation statements used in the evaluation of historical and runtime data.

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 9-1](#).

Table 9-1 Multiple Conditions

Condition 1	Condition 2	Rule Result
True	True	True
False	False	False - Rule is not triggered
True	False	False
False	True	False

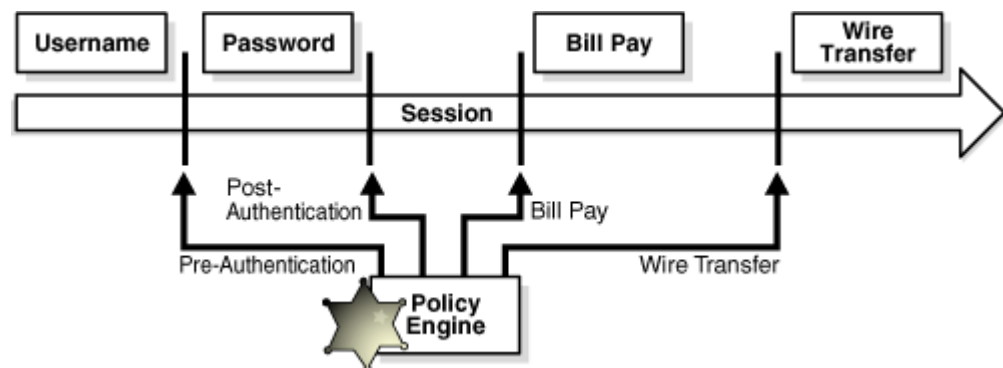
For information on the conditions available in the system, see [Appendix B, "Conditions Reference."](#)

9.1.4 Checkpoints

The checkpoint is a decision and enforcement point when policies are called 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.

Figure 9-2 Checkpoints



Out-of-the-box checkpoints are listed in [Table 9-2](#).

Table 9-2 Out of Box Checkpoints

Condition	Description
System CC Challenge	The policy is run for the Ask Question flow.
Registration	The policy is run to check the registration of user.
Preferences	The policy is run when preferences page is displayed after login.

Table 9–2 (Cont.) Out of Box Checkpoints

Condition	Description
Forgot Password	The policy is run for forgot password flow
Challenge	The policy is run whenever a challenge is invoked
In-session	The policy is run anytime during a transaction.
Pre-authentication	After the user enters a user name, the policy is run to perform basic security checks
Post-authentication	After the user is authenticated, the policy is run to block, challenge, or allow. Registration is run after allow.

Examples of possible checkpoints during a session are listed as:

- Bill pay
The policy is executed during a bill pay.
- Wire transfer
The policy is executed when the user is on a wire transfer page.

Bill pay and Wire transfer are used as examples of possible points during a session. They are not available in Oracle Adaptive Access Manager out of the box.

Checkpoint Example

A fraudster has stolen a user's username 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 anonymizing proxy to mask the location, a challenge might occur during Post-Authentication. When the fraudster fails to provide the correct answers, fraud is prevented.

9.1.5 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, Username, Location, Device, Action, and Alert.

9.1.6 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 10, "Managing Groups."](#)

9.1.7 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 10, "Managing Groups."](#)

9.1.8 User Group Linking

You can specify for policies to execute for all users or a selected user group through Run mode.

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.

9.1.9 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.

9.1.10 Trigger Combinations and Triggers

Rules are triggered when their conditions all evaluate to true.

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 9.12, "Working with Trigger Combinations."](#)

For an example of setting up a trigger combination, see [Section 9.32.7, "Use Case: Trigger Combination."](#)

9.1.11 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.

9.1.12 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."

9.1.13 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 12, "Using the Scoring Engine."](#)

9.1.14 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 determine the score for the checkpoint. The default scoring engine at the checkpoint level is "Maximum."

For more information on the scoring engine, see [Chapter 12, "Using the Scoring Engine."](#)

9.1.15 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.

9.1.16 Policy Type

The concept of policy type has been removed from the product.

Only security policies are available in 11g. Although policy types for the 10g policies will be retained in the OAAM database, OAAM 11g will ignore the policy types of Business, Third-party, and Workflow in the database and treat all policy types as "Security" policies for all purposes.

Since there are no policy types, the policy type scoring engine will be ignored and the scoring engine at the checkpoint level will be applied for all policies.

9.2 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 9.24, "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 12, "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 Process."](#)

5. Build alert and action groups so that they are available when you build the policy.

For information, see [Section 10.9, "Creating a Group."](#)

6. Create the policy.

For information, see [Section 9.8, "Creating Policies."](#)

9.3 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 12, "Using the Scoring Engine."](#)

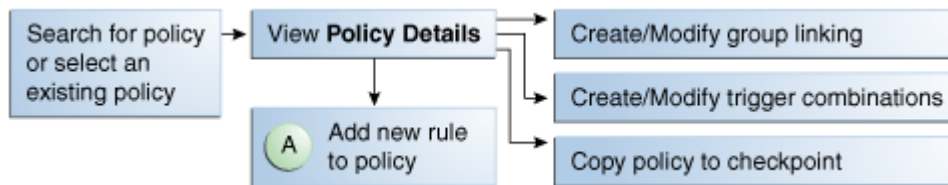
4. Add the required rules with the conditions to the policy and use trigger combinations to determine the order of rule to be triggered.

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.

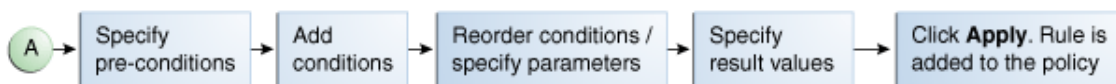
Figure 9–3 Overview of Creating a Policy



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 9–4 Overview of Adding a New Rule



9.4 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 9–5, "Policies Search Page"](#).

Figure 9–5 Policies Search Page

Search for the policy or click the New Policy button to create a new policy.

Search Filter:

- Checkpoint: -- Select --
- Policy Name:
- Policy Status: -- Select --
- Run Mode: -- Select --
- Linked Groups: -- Select --
- Create Time: -
- Update Time: -

Buttons: Search, Reset, Save...

Search Results

Row	Policy Name	Policy Status	Checkpoint	Run Mode	Linked Groups	Create Time	Update Time	Description
1	Challenge	Active	Challenge	All Users		6/4/2010 2:59 PM	6/4/2010 3:04 PM	Challenge options policy
2	Post Authentication Security	Active	Post-Authentication	All Users		6/4/2010 2:59 PM	6/4/2010 2:59 PM	Post Authentication Security Policy.
3	Pre Authentication Block	Active	Pre-Authentication	All Users		6/4/2010 2:59 PM	6/4/2010 2:59 PM	This model stops fraudulent login attempts before the
4	Pre Authentication Flow	Active	Pre-Authentication	All Users		6/4/2010 2:59 PM	6/4/2010 2:59 PM	Pre-Auth model to identify user authentication client ty
5	Registration	Active	Registration	All Users		6/4/2010 2:59 PM	6/4/2010 2:59 PM	Registration
6	Risky IP nested model	Active	Post-Authentication	Linked Users		6/4/2010 2:59 PM	6/4/2010 2:59 PM	These rules will run for a user that has questions active
7	System CC Challenge	Active	CSR KBA Challenge	All Users		6/4/2010 2:59 PM	6/4/2010 2:59 PM	Customer care challenge model
8	System Forgot Password	Active	Forgot Password	All Users		6/4/2010 2:59 PM	6/4/2010 2:59 PM	This model contains rules which can block the logins
9	System preferences	Active	Preferences	All Users		6/4/2010 2:59 PM	6/4/2010 2:59 PM	Checks to see if a user is registered.

Rows Selected: 1 | Total Rows: 9

9.5 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 9–3](#).

Table 9–3 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.
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. <ul style="list-style-type: none"> ■ 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.
Create Time	Time when policy was created.
Update Time	Time when policy was last updated.

9.6 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.

9.7 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.

9.8 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.

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 will not remove it from the system. You will be 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 9.1.4, "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 12, "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 9.15, "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 9.11, "Adding a New Rule"](#)).

When you add a rule, you can specify:

- **Preconditions.** For information, see [Section 9.20.2, "Specifying Preconditions."](#)
- **Conditions.** For information, see [Section 9.25, "Adding Conditions to a Rule."](#)
- Order of conditions/parameter values
- **Results.** For information, see [Section 9.20.3, "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 9.9, "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 9.12, "Working with Trigger Combinations."](#)

9.9 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.

You can select whether to link the policy to all users of all applications, 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. 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.

9.9.1 Linking a Policy to All Users

If you want a policy to be applied to all users, follow these steps:

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 **All Users**.

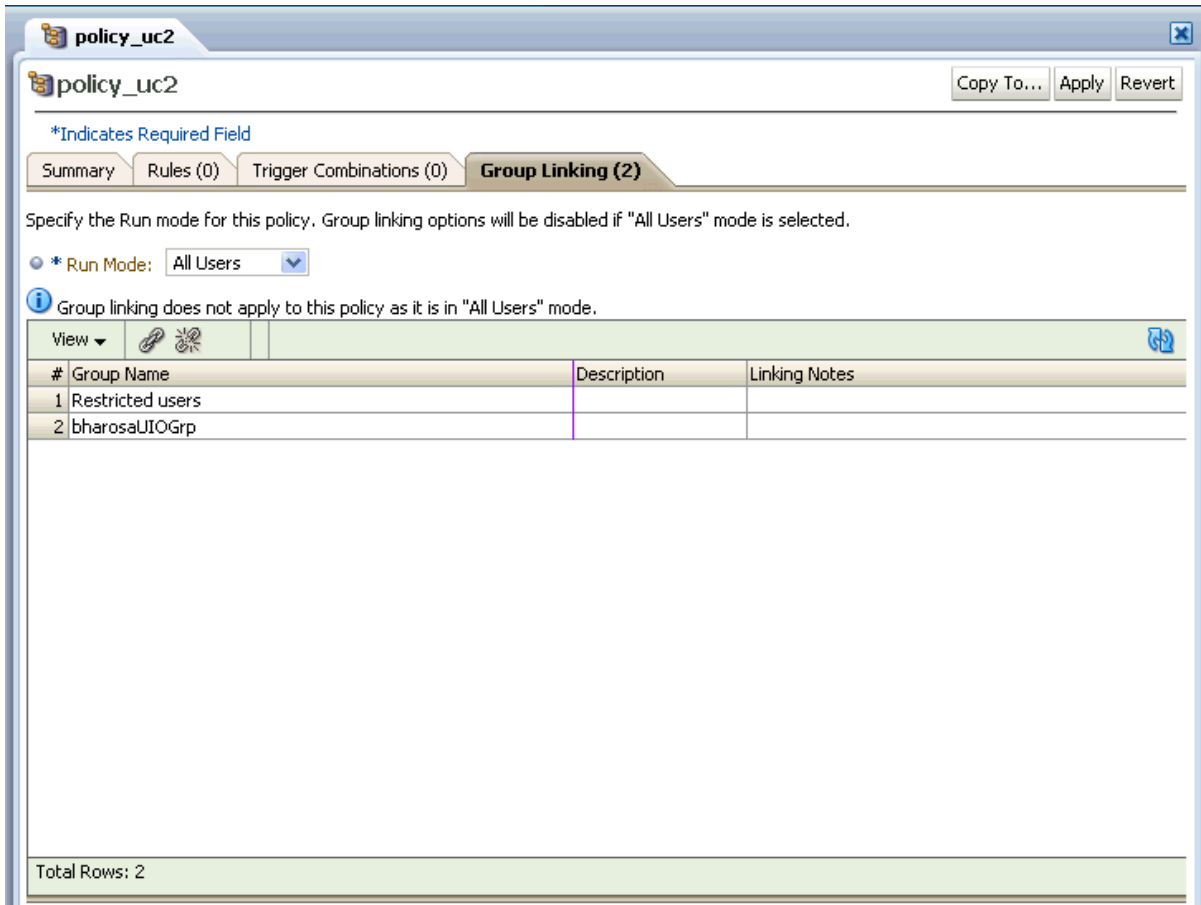
Since **All Users** is specified, all group linking options and the table are disabled.

4. Click **Apply** to save the changes.

Changes are applied to the policy.

If **Revert** is clicked, the changes are discarded.

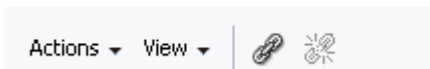
Figure 9–6 Policy Linked to All Users



9.9.2 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**.

9.10 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 9.5, "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 9–7, "Policy Details Summary Tab"](#).

Figure 9–7 Policy Details Summary Tab

The screenshot shows a web interface for editing a policy. The browser window title is "Policies" and the page title is "policy_pjlee_082709". The page has a navigation bar with "Copy To...", "Apply", and "Revert" buttons. Below the navigation bar, there are tabs for "Summary", "Rules (0)", "Trigger Combinations (0)", and "Group Linking (0)". The "Summary" tab is active and displays the following fields:

- * Policy Name: policy_pjlee_082709
- * Policy Type: Security
- * Policy Status: Active
- * Checkpoint: Pre-Authentication
- * Scoring Engine: Average
- * Weight: 100
- * Description: verify procedures

Table 9–4 Policy Details Summary Tab

Field	Description
Policy Name	Name of the policy.
Policy Status	Status of the policy: Active or Disabled.
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.

9.11 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](#)

9.11.1 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 9–8 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.

9.11.2 Specifying General Rule Information

Table 9–5, "New Rule Page" summarizes the general information of a rule.

Table 9–5 *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.

9.11.3 Configuring Preconditions

To configure preconditions for the rule, follow the procedure in [Section 9.20.2, "Specifying Preconditions."](#)

Through preconditions, you can specify the group to exclude and the geolocation confidence factor parameters.

9.11.4 Adding Conditions

To add conditions for the rule, follow the procedure in [Section 9.25, "Adding Conditions to a Rule."](#)

9.11.5 Specifying Results for the Rule

To specify the results for if the rule triggers, follow the procedure in [Section 9.20.3, "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 10, "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 10, "Managing Groups."](#)

9.11.6 Adding or Copying a Rule to a Policy

The **Copy Rule** button enables you to copy an existing rule to other policies.

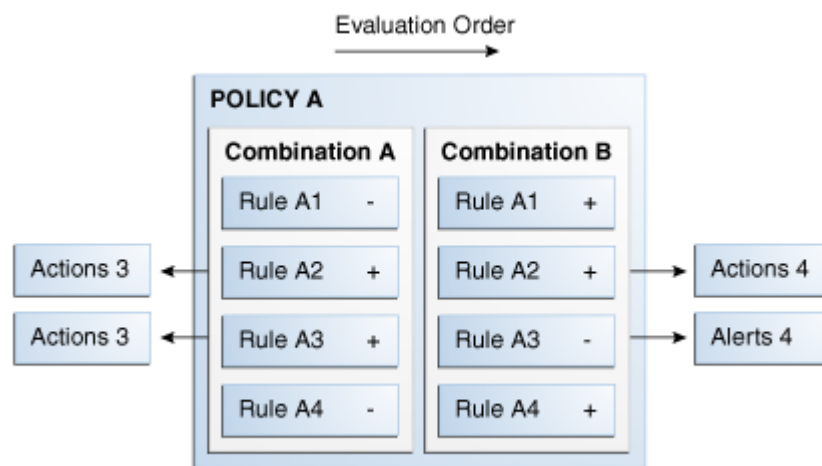
9.12 Working with Trigger Combinations

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.

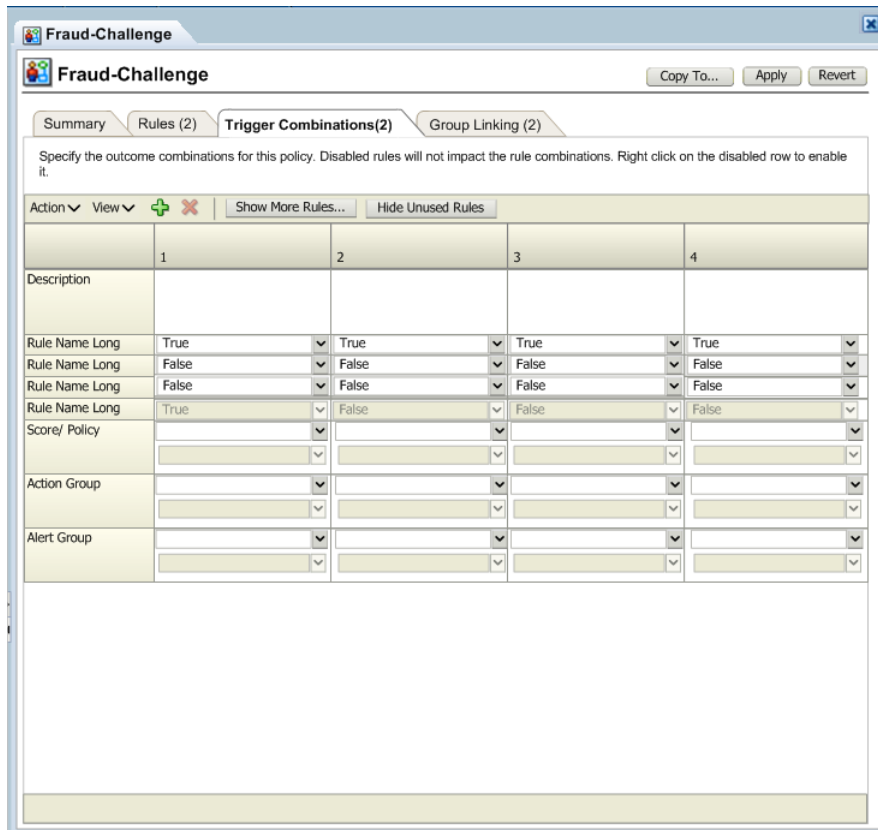
The trigger combinations evaluate sequentially, stopping as soon as a trigger combination is matched.

Figure 9–9 *Trigger Combination Structure*



Trigger Combinations can be accessed through the **Rule Details** page. Each column in the table corresponds to a trigger combination.

Figure 9–10 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 10, "Managing Groups."](#)

Table 9–6 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. Scores of 0 or less than 0 will be ignored. If you select Policy, a policy list appears with policies of same checkpoint.
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 9–7, "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 9–7 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.

9.12.1 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.

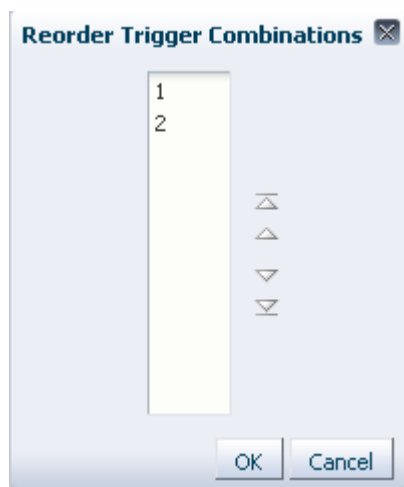
If you navigate away from the tab while editing trigger combinations, the unsaved trigger combinations are saved in the session and available when you navigate back.

9.12.2 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**.

9.12.3 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**.

9.13 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 9.5, "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**.
5. In the information screen, click **OK**.

An information screen appears.

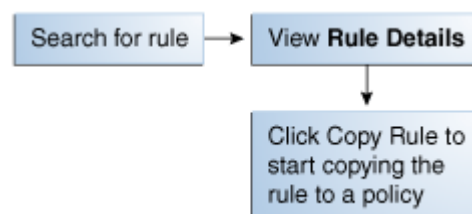
The policy deleted successfully.

You cannot undo the delete. The changes are permanent.

9.14 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 9–11 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.

9.15 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 9–8, "Copy Policy to Checkpoint"](#) lists the fields in the **Copy Policy** screen.

Table 9–8 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 <i>policy_name</i> Copy. You can edit the policy name, if needed.
Status	The policy status of "disabled" is set as the default value.
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.

9.16 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.

9.16.1 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**.

9.16.2 Importing a Policy

Note for Policies Migrated from 10g to 11g

Only security policies are available in 11g. Business, third-party, workflow policy types have been removed from Oracle Adaptive Access Manager.

In 10g, scoring was not used by business policies. In 11g, 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 11g onward.

To import policies:

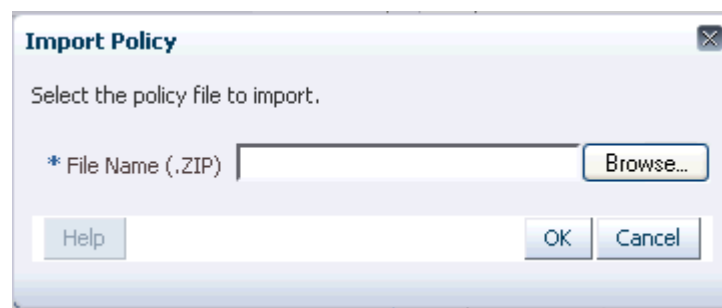
1. Create a `\tmp` folder in the drive where you have installed Weblogic if OAAM Admin is installed on the Windows platform.

For example, if the Weblogic domain is on the C drive, you would create a `c:\tmp` folder.

This folder will be 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 9–12 *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.

9.17 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 9–13, "Rules Search Page"](#).

Figure 9–13 Rules Search Page

Use the search tool to find Rules

Search Advanced Saved Search Search Rules

Match All Any

Policy Name Rule Status -- Select -- Rule Type -- Select --

Rule Name Description Checkpoint -- Select --

Search Reset Save...

Search Results

View Refresh

Policy Name	Checkpoint	Rule Name	Rule Type	Rule Status	Score	Weight	Acti
<input type="checkbox"/> 000PreAuth	Pre-Authentication	00test	User	Active	1000	100	Bloc
<input type="checkbox"/> 201 Cookie enable ch	Device Identification	Is Flash Cookie Disabl	Device ID rules	Active	0	100	
<input type="checkbox"/> 201 Cookie enable ch	Device Identification	Is Secure Cookie Disa	Device ID rules	Active	0	100	
<input type="checkbox"/> 202 Flash missing	Device Identification	Is flash cookie enable		Active	1000	100	
<input type="checkbox"/> 203 Cookie missing	Device Identification	Is secure cookie enat		Active	1000	100	
<input type="checkbox"/> 204 Http header mism	Device Identification	Browser mismatch	Device ID rules	Active	1000	100	
<input type="checkbox"/> 204 Http header mism	Device Identification	Browser upgraded	Device ID rules	Active	1000	100	
<input type="checkbox"/> 204 Http header mism	Device Identification	Header mismatch high	Device ID rules	Active	1000	100	
<input type="checkbox"/> 204 Http header mism	Device Identification	Known hdr mismatch	Device ID rules	Active	1000	100	
<input type="checkbox"/> 204 Http header mism	Device Identification	OS Mismatch	Device ID rules	Active	1000	100	
<input type="checkbox"/> 204 Http header mism	Device Identification	OS Upgraded	Device ID rules	Active	1000	100	
<input type="checkbox"/> 205 Hdr mismatch No	Device Identification	Browser mismatch	Device ID rules	Active	1000	100	
<input type="checkbox"/> 205 Hdr mismatch No	Device Identification	Browser upgraded	Device ID rules	Active	1000	100	
<input type="checkbox"/> 205 Hdr mismatch No	Device Identification	Header mismatch high	Device ID rules	Active	1000	100	
<input type="checkbox"/> 205 Hdr mismatch No	Device Identification	Is Flash Cookie Enabl		Active	1000	100	
<input type="checkbox"/> 205 Hdr mismatch No	Device Identification	Known hdr mismatch	Device ID rules	Active	1000	100	
<input type="checkbox"/> 205 Hdr mismatch No	Device Identification	OS Mismatch	Device ID rules	Active	1000	100	
<input type="checkbox"/> 205 Hdr mismatch No	Device Identification	OS Upgraded	Device ID rules	Active	1000	100	

Total Rows 141

9.18 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 9–9 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.

Table 9–9 (Cont.) Rules Results

Field	Description
Rule Description	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.

9.19 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.

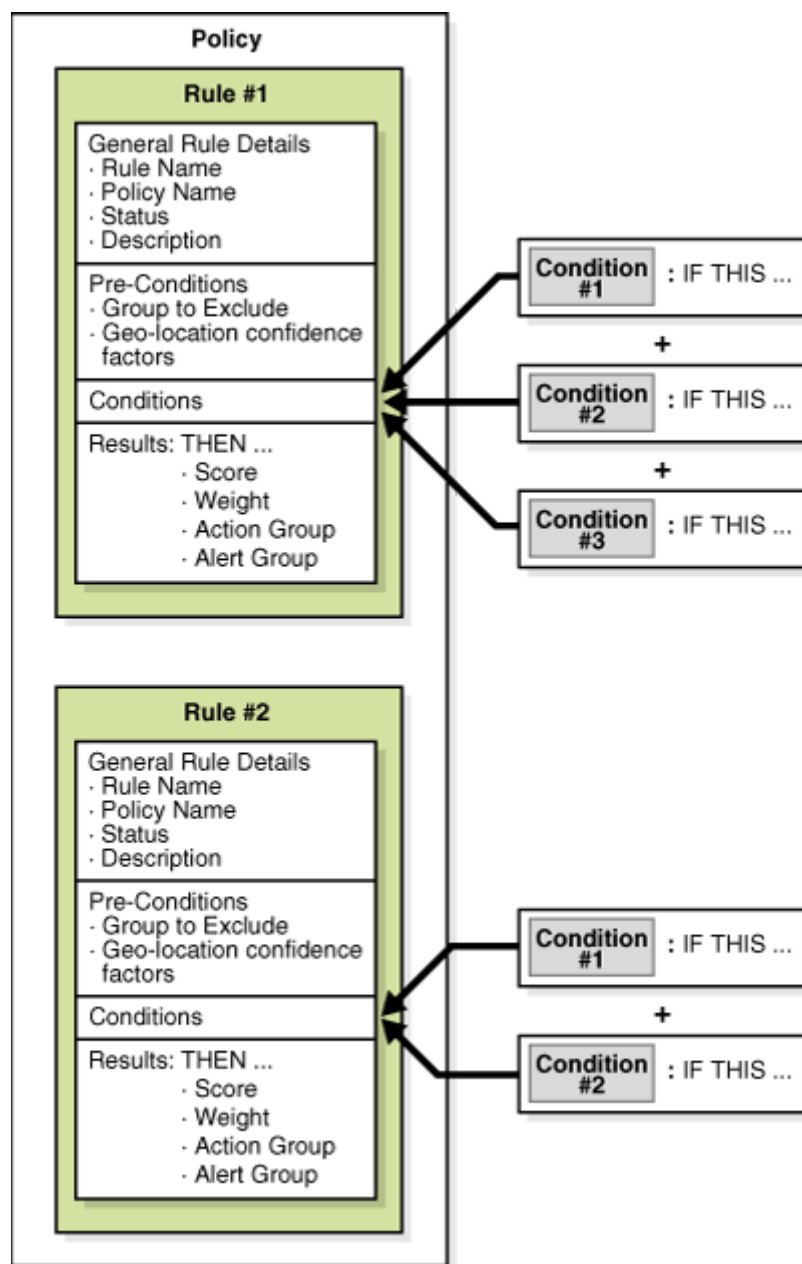
The **Rule Details** page has four tabs

- General
- Preconditions
- Conditions
- Results

These tabs allow the management of the rule.

[Figure 9–14](#) illustrates the tabs in the Rule Details page and the information to enter for each tab.

Figure 9–14 Policies



9.20 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.

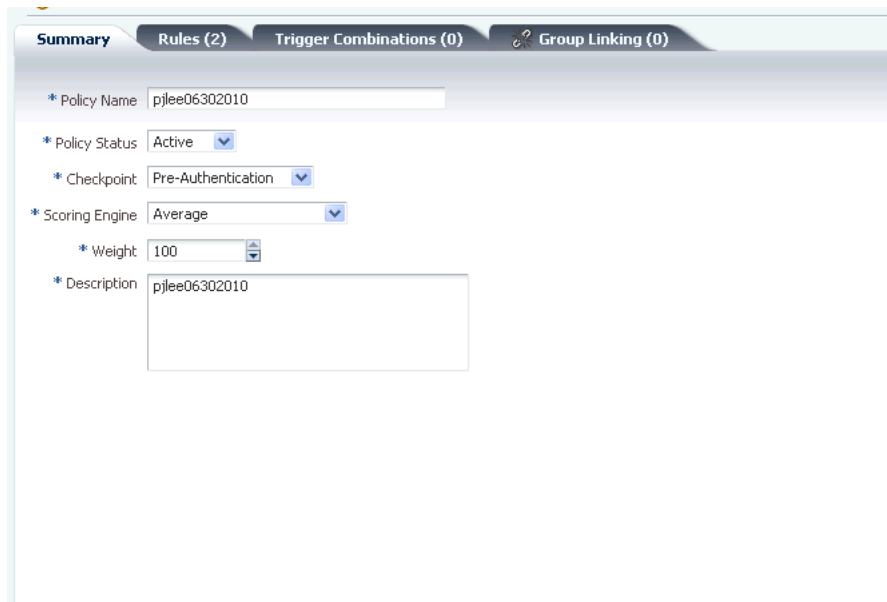
The total number of conditions in the rule appears in parenthesis next to the Conditions tab title.

4. Edit the rule's general information (Section 9.20.1, "Modifying the Rule's General Information").
5. Edit the Preconditions (Section 9.20.2, "Specifying Preconditions").
6. Edit/Add Conditions (Section 9.25, "Adding Conditions to a Rule").
7. Edit the Results (Section 9.20.3, "Specifying the Results for a Rule").
8. Click **Apply** to save the changes or **Revert** to discard them.

9.20.1 Modifying the Rule's General Information

From the **Summary** tab, you can modify the rule name, status, and description.

Figure 9–15 Rule Details Summary Tab



The fields displayed are listed in Table 9–10.

Table 9–10 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.

9.20.2 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 be 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, geo-location 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.

9.20.3 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 9–11 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.

9.21 Working with Scores and Weights

For information about the processing of policies to come up with scores, actions, and alerts, see [Chapter 12, "Using the Scoring Engine."](#)

9.22 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 with 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 rows are deleted in the trigger combinations where this rule was used.
5. When the confirmation appears, click **OK**.

9.23 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 B, "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 9–12, "Conditions Search fields"](#) lists the fields in the Search section.

Table 9–12 *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.

9.24 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.

9.25 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 9–16 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 9–17 Add Conditions

Search and select the conditions that you want to add to the rule

Search Search Conditions

Condition Name Type Context Data

Description Checkpoint

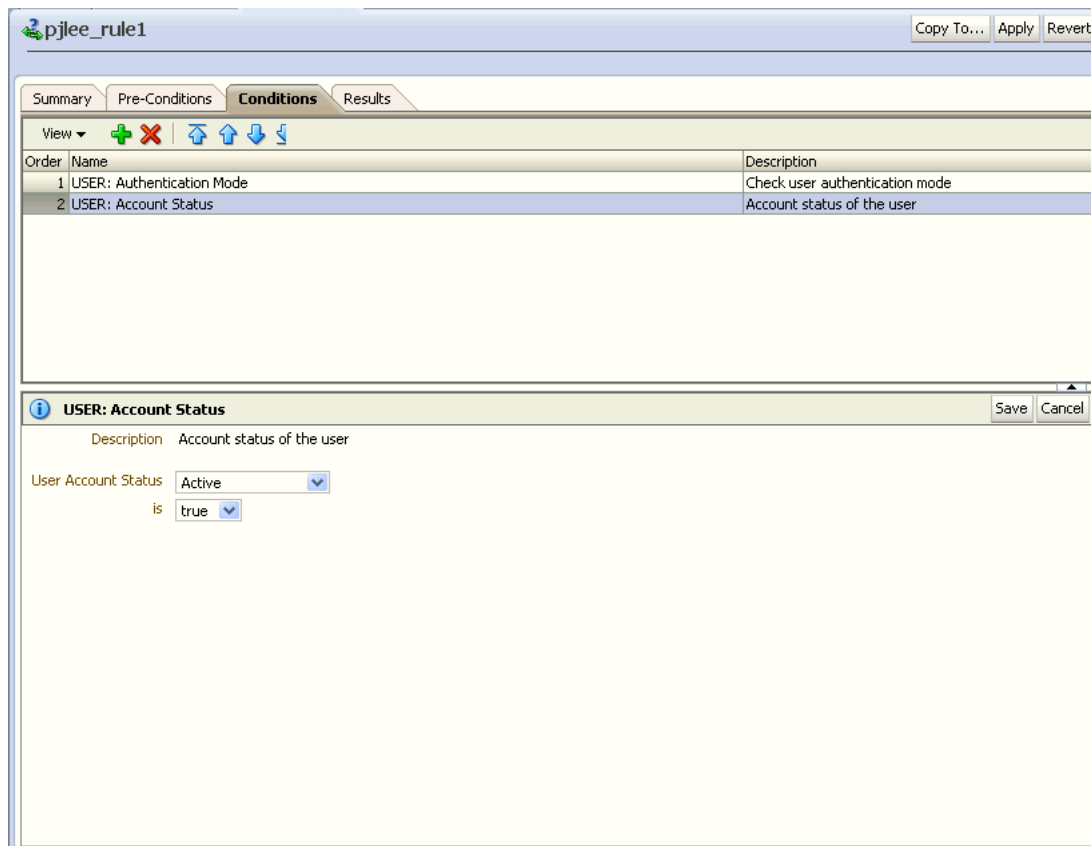
Results

View

Condition Name	Type	Description
1 User: Account Status	User	Account status of the user

Rows Selected 1

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 9–18, "Condition Parameters"](#).

Figure 9–18 Condition Parameters

The top subtab displays the conditions in the rule.

[Table 9–13](#) lists the fields in the top subtab of the **Conditions** tab.

Table 9–13 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.

9.26 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.

9.27 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**.

9.28 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 9.29, "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.

9.29 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.

9.30 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.

9.31 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.

9.32 Use Cases

This section describes example use cases for policies and rules.

9.32.1 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 10.12, "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.

9.32.2 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 named 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 will be added to the system or it will overwrite/update 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.

9.32.3 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 9.1.4, "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 12, "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 9.9, "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 9.11, "Adding a New Rule"](#)) or by copying an existing one ([Section 9.14, "Copying a Rule to a Policy"](#)) to the policy.

9.32.4 Use Case: Add New Rule

After you have created a security policy (see [Section 9.32.3, "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 versus 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 than 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.

Summary

Rules

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.

9.32.5 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 [Section 9.32.2](#), "Use Case: Import Policy."

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.

9.32.6 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 will trigger 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.

9.32.7 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 [Section 9.32.3, "Use Case: Create a Policy."](#)

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 will be 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.

9.32.8 Use Case: Trigger Combination and Rule Evaluation

Jeff, a Security Admin, 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 will trigger if the user has registered questions and he has logged in from time bucket less than 10% of time. The Result, he will be 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 14, "Managing Autolearning."](#)

9.32.9 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 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.
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**.

9.32.10 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.

9.32.11 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**.

9.32.12 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.

9.32.13 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 9.9, "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**.

9.32.14 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.

9.32.15 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.

9.32.16 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.

9.33 Best Practices

This section outlines some best practices for using policies, rules, and conditions.

9.33.1 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.

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.

10.1 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 will use this group.

10.2 Group Types

The following types of groups are available:

Table 10–1 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 10–1 (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 device 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.
Username	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." Username may not be unique across applications. The unique combination would be the Organization ID with the Username.
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 10–1 (Cont.) Group Types

Type	Description
Top-Level Domains	<p>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).</p> <p>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.</p>
Transaction Status	<p>This group contains the status of the user when a transaction is being performed.</p> <p>This is an enum group type.</p>
User ID	<p>This group contains User IDs. The customer uses a scheme to uniquely identify users.</p> <p>The User ID may not be unique across applications. The unique combination would be the Organization ID with the User ID.</p> <p>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.</p>

10.3 Group Usage

Groups are used in the following items:

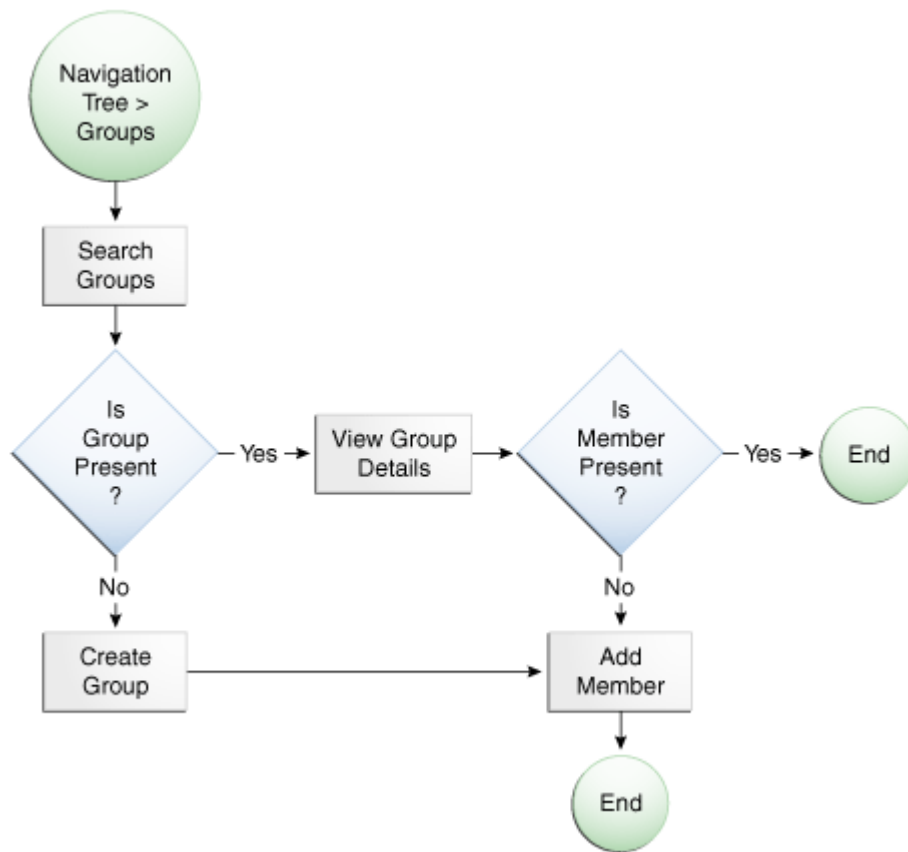
- Policies
 - A policy is linked to a User ID group or all users and members of the user group or all users that are evaluated.
 - The Policy Tree shows the linking of User ID groups to policies.
- Rules within policies
 - OAAM Admin applies rules on specified users, devices, or location groups to evaluate 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 will take 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.

10.4 User Flows

In the create and edit user flow, you will 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 defining a group.

As an example user flow, the group creation flow, is shown in [Figure 10–1](#).

Figure 10–1 Group Creation Flow



10.5 Navigating to the Groups Search Page

From the **Groups Search** page, you can search, view, create, import, export, and delete groups.

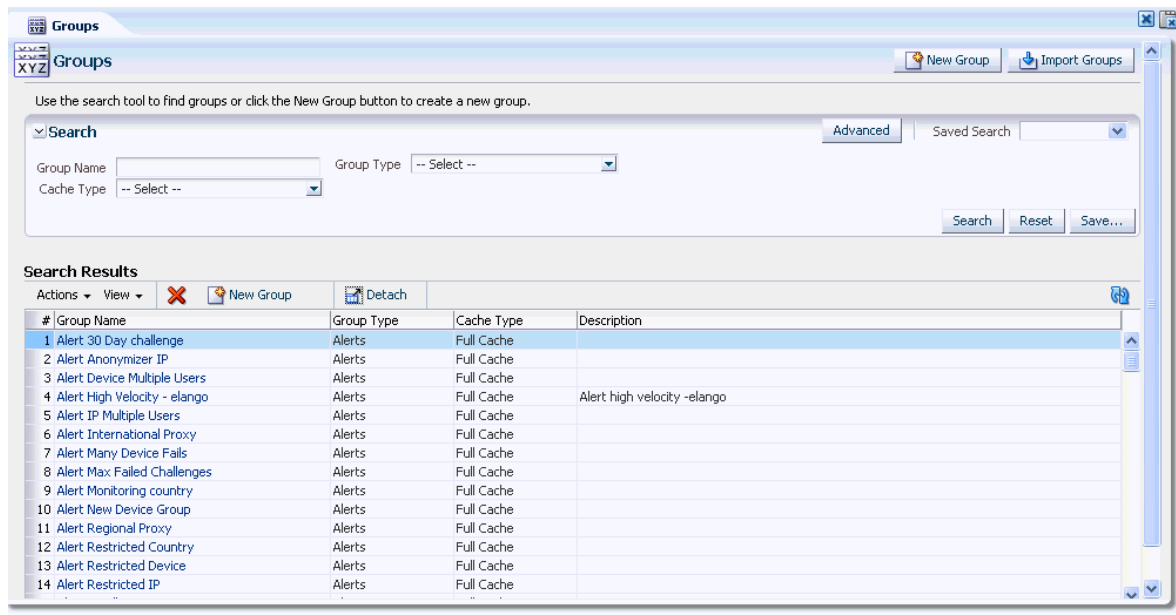
To open the **Groups Search** page:

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, "Access to 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 10–2 Groups Search page



10.6 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 10.5, "Navigating to the Groups Search Page."](#)
2. Specify criteria to locate the group and click **Search**.

Clicking **Reset** instead of **Search** will reset the search criteria.

Search parameter values are not required. If you choose to leave the fields blank, all groups will display in your search results.

The search filters are described in [Table 10–2](#).

Table 10–2 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 10–1

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.

10.7 Viewing Details about a Group

The **Group Details** tab has summary and member tabs.

To view details about a group:

1. Navigate to the **Groups Search** page, as described in [Section 10.5, "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 will have a member tab labeled **User ID**.

The members tab shows all the members of the group. The members tab will typically show member name/ ID, description, and any other critical attributes of members. The exact information will differ depending on the group type.

Note: You cannot edit existing **Action** elements and their properties.

10.8 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 10–3 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

10.9 Creating a Group

The process for creating a group involves:

1. [Defining a Group](#)
2. [Adding Members to a Group](#)

10.9.1 Defining a Group

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, "Access to Search, Create, and Import."](#)

The **New Group** screen is displayed.

3. In the **New 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 10-1](#)

Figure 10-3 *New Group screen*

5. Set the cache policy to **Full Cache** or **None**.
The **Cache Policy** is set to **None** automatically.

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.

10.9.2 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 will depend on the group type. Refer to the following tables for the appropriate procedure for the group you are creating.

When you search for members, the ones that are already part of your group will not be available in your search results.

Note: The server must be restarted for the elements you add to take effect.

Create a new member to add to the group (no search/ filter option)

[Table 10–4](#) lists groups that add members without an option to search or filter.

If you are adding members to a group listed in [Table 10–4](#), see [Section 10.10, "Creating a New Element/Member to Add to the Group \(No Search and Filter Options\)."](#)

Table 10–4 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 10–5](#) 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 10–5](#), see [Section 10.11, "Filtering an Existing List to Select an Element to Add to the Group \(No Creation of a New Element\)."](#)

Table 10–5 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 10–6](#) 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 10–6](#), see [Section 10.12, "Searching for and Adding Existing Elements or Creating and Adding a New Element."](#)

Table 10–6 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 10.13, "Adding Alerts to a Group."](#)

Search and add existing elements only (No Creation)

[Table 10–7](#) 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 10–7](#), see [Section 10.14, "Searching for and Adding Existing Elements."](#)

Table 10–7 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

10.10 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 will be added to the group.

Table 10–8 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.

10.11 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.

10.11.1 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 will be 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 will be 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.

10.11.2 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 will be 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.

10.11.3 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.

10.12 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
- Username
- IP
- Internet Service Provider

When you search for members, the ones that are already part of your group will not be available in your search results.

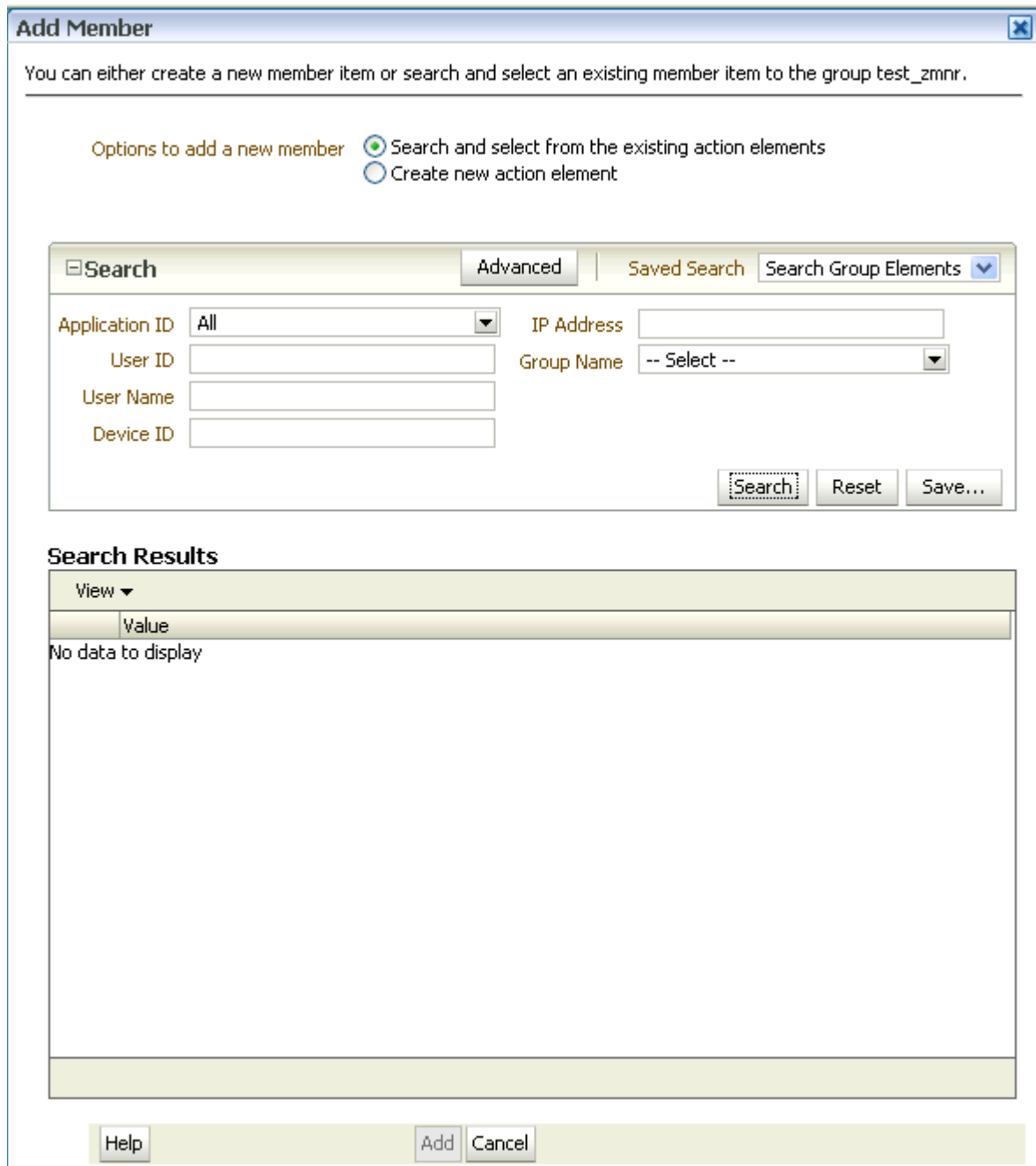
Because the procedures for alert groups are different from the other groups listed earlier, separate sections are provided.

10.12.1 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 10–4 Search and Select Member



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.

10.12.2 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 10–5 Add Member

3. Type in the values for the member.

Table 10–9 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.

10.13 Adding Alerts to a Group

Procedures for adding alerts to an alert group are provided in the following sections.

10.13.1 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**.
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 will not propagate to the other alerts.

10.13.2 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 10–10 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 **Info**.
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 10–6 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.

10.14 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 will not be 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.

10.14.1 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.

10.14.2 Adding Actions to an Action Group

Follow these steps for adding actions to an action group:

10.14.2.1 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 10–7 Search for an Action

Add Member

You can either create a new member item or search and select an existing member item to add to the group pjlee_action.

Options to add a new member Search and select from the existing elements
 Create new element

Search Basic Saved Search GroupEnumElemListCriteria

Name Group

Description

Search Reset Save... Add Fields

Search Results

View

	Name	Description
1	Reset User Questions	Reset User Questions
2	Add to User watch list	Add to User watch list
3	Register Image Textp	Register Image Textpad the user
4	OTP challenge Email	Challenge user using OTP via Email
5	Register Questions H	Register Questions HTML the user
6	Password Keypad Alp	Password Keypad Alpha Turk Generic First-Time the user
7	OTP challenge SMS	Challenge user using OTP via SMS
8	Register User Keypac	Register User Keypad Full the user
9	Locked	Locked the user because of challenge question
10	Password Textpad Ge	Password TextPad Generic FirstT ime the user
11	Partial Password	Challenge user using Partial Password
12	Register User Option	Register User Optional Question Pad the user
13	Add to IP watch list	Add to IP watch list
14	Add to User Black list	Add to User Black list
15	Device by digital cook	Use digital or flash cookie device

Help Add Cancel

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.

10.14.2.2 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 will not have any effect on applications directly.

10.15 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 10–11, "Editing a Member of a Group"](#).

1. Navigate to the **Groups Search** page, as described in [Section 10.5, "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 10–11 *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

10.16 Removing Members of a Group

To remove members of a group:

1. Navigate to the **Groups Search** page, as described in [Section 10.5, "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.

10.17 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 10.5, "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.

10.18 Exporting and Importing a Group

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

10.18.1 Exporting a Group

To export a group:

1. Navigate to the **Groups Search** page, as described in [Section 10.5, "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.

10.18.2 Importing a Group

To import a group:

1. Navigate to the **Groups Search** page, as described in [Section 10.5, "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 will be updated/overwritten. If the file contains groups with names that do not exist, the groups will be added to the system.

If you are importing a delete script, the groups will be deleted from the system.

If you try to import groups in an invalid format, an error will be displayed.

10.19 Deleting Groups

To delete groups:

1. Navigate to the **Groups Search** page, as described in [Section 10.5, "Navigating to the Groups Search Page."](#)
2. In the **Groups Search** page, search for a specific group or a list of groups you're 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.

10.20 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 10.18.1, "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 10.18.2, "Importing a Group."](#)

10.21 Use Cases

This section describes example use cases for groups.

10.21.1 Use Case: Migration of Groups

Chuck is an Administrator migrating a 10.1.4.5 deployment to 11g 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 11g 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**.

10.21.2 Use Case: Create Alert Group and Add Members

The velocity rule you created (in [Section 9.32.4, "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.

10.21.3 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 **Username** field, enter Phillip's username.
 - c. In the **Alert Level**, select **High**.

There are no other high severity security alerts.

For information on Phillips' security alerts, see [Section 5.5.2, "Use Case: Session Details Page."](#)

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.

10.21.4 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**.

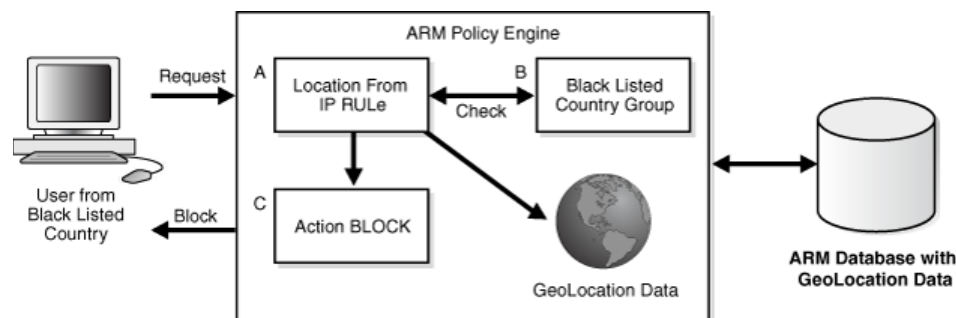
The **Add Conditions** page is displayed where you can search for and select the **Location: In Country Group** condition and add it to the rule.

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 10–8 Black-Listed Countries



10.21.5 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.

10.21.5.1 Create Country Blacklist Policy (1): Create Fraudulent Country Policy and Rule

You must first create a Fraudulent Country policy with the following attributes:

Table 10–12 *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"

10.21.5.2 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 10–13 *Country Group*

Attribute	Value
Group Name	Country_Blacklist
Group Type	Countries
Cache Policy	Full Cache
Description	OAAM Country Blacklist Group

10.21.5.3 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 10–14 *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

10.21.5.4 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 10–15 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.

10.21.5.5 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.

10.21.6 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."

10.21.7 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.

10.21.8 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 etc.
- **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.

10.21.9 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.

10.22 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.
- Ensure that the caching is set to "Full Cache" for action and alert groups.

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:

- [Introduction and Concepts](#)
- [Navigating to the Policy Set Details Page](#)
- [Viewing Policy Set Details](#)
- [Editing a Policy Set](#)
- [Adding or Editing an Action Override](#)
- [Adding or Editing a Score Override](#)
- [Use Cases](#)
- [Best Practices for the Policy Set](#)

11.1 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:

- [Policy Set](#)
- [Action and Score Overrides](#)

11.1.1 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.

11.1.2 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 will be generated if the checkpoint risk score falls between 500 and 1000.

11.1.3 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."

```
crypt.tracker.rules.allowControlledActions
```

11.2 Navigating to the Policy Set Details Page

Only one policy set is available.

To access the **Policy Set Details** page:

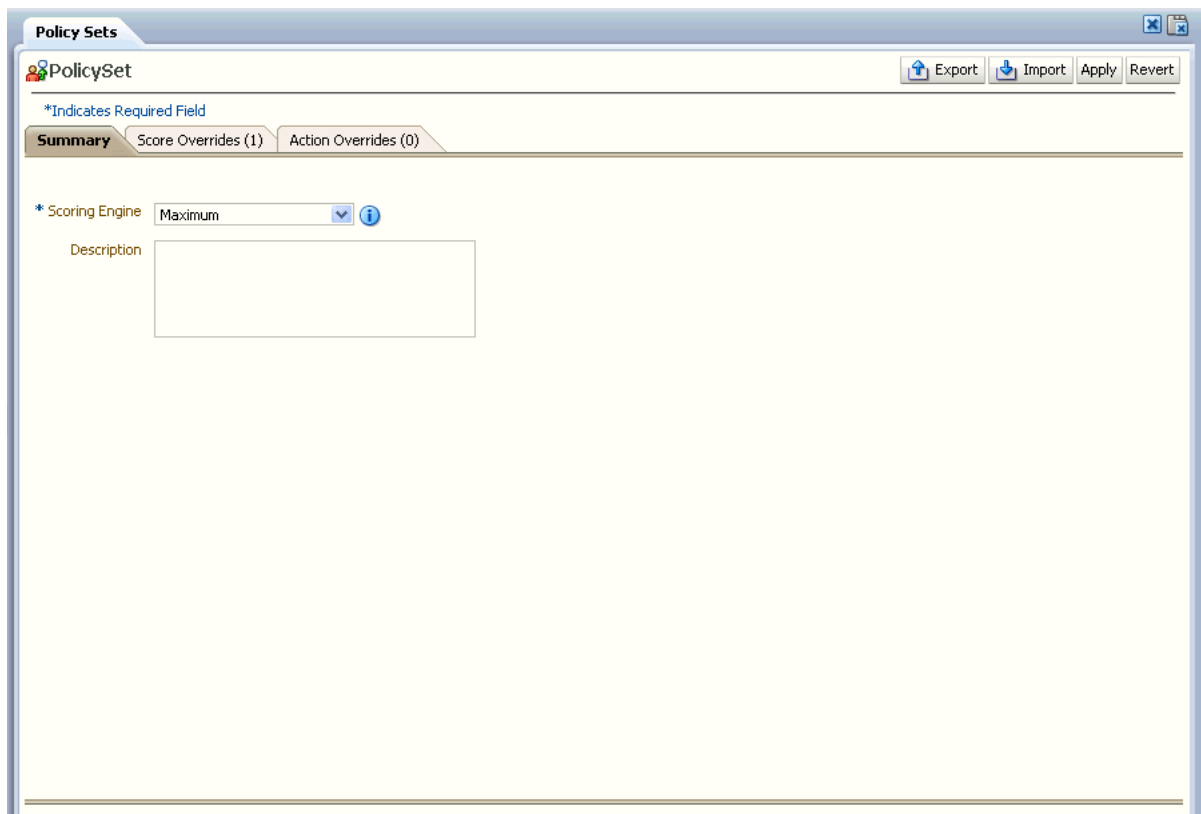
1. Expand the Navigation tree.
2. From the Navigation tree, select **Policy Set**.

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.

Figure 11–1 Policy Set Details



11.3 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

11.4 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** screen appears.

Figure 11–2 Add Score Override

The screenshot shows a web-based interface for managing Policy Sets. A modal dialog box titled "Add Score Override" is open. The dialog contains the following fields and controls:

- Checkpoint:** A dropdown menu with "Pre-Authentication" selected.
- Minimum Score:** A text input field containing "0".
- Maximum Score:** A text input field containing "1000".
- Action Group:** A dropdown menu with "-- Select --" selected.
- Alert Group:** A dropdown menu with "-- Select --" selected.

At the bottom of the dialog, there are four buttons: "Help", "Apply", "Revert", and "Cancel".

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**.

11.5 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** screen appears.

Figure 11–3 Add Action Override

The screenshot shows the 'Add Action Override' dialog box within the 'Policy Sets' application. The dialog box is titled 'Add Action Override' and contains the following fields:

- * Checkpoint: Pre-Authentication (dropdown menu)
- From Action: -- Select -- (dropdown menu)
- To Action: -- Select -- (dropdown menu)
- Alert Group: -- Select -- (dropdown menu)
- Duration (Minutes): 0 (spin box)
- * Count: 1 (spin box)

Buttons for 'Help', 'Apply', 'Revert', and 'Cancel' are located at the bottom of the dialog box.

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 will stop blocking people and start 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 will be 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 will continue to be block in the specified duration instead of being challenged.

10. Click **Apply**.

11.6 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 12, "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 11.4, "Adding or Editing a Score Override."](#)
4. To edit the action overrides, follow the instructions in [Section 11.5, "Adding or Editing an Action Override."](#)

11.7 Use Cases

This section describes example use cases for using policy set.

11.7.1 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 will be triggered for immediate attention by the fraud investigators and the users will be "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 will 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**

11.7.2 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 will be triggered for immediate attention by the fraud investigators and the users will be "blocked instead of being "challenged." But there are about 10 training folks and they are given temp allow for the next 1 week. How will 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 will 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.

11.8 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 will not be broken when they are imported back into a system.

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 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.

12.1 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.

12.1.1 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.

12.1.2 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.

12.1.3 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.

12.1.4 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 10g to 11g

Only security policies are available in 11g. Business, third-party, workflow policy types have been removed from Oracle Adaptive Access Manager.

In 11g, all policies will be treated as security policies.

12.1.5 Policy Type

The concept of policy type has been removed from the product. All policies are treated as security policies in 11g.

12.1.6 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.

12.1.7 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.

12.1.8 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 determine the score for the checkpoint. The default scoring engine at the checkpoint level is "Aggregate."

Table 12–1 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.

12.2 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 12-1**, 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

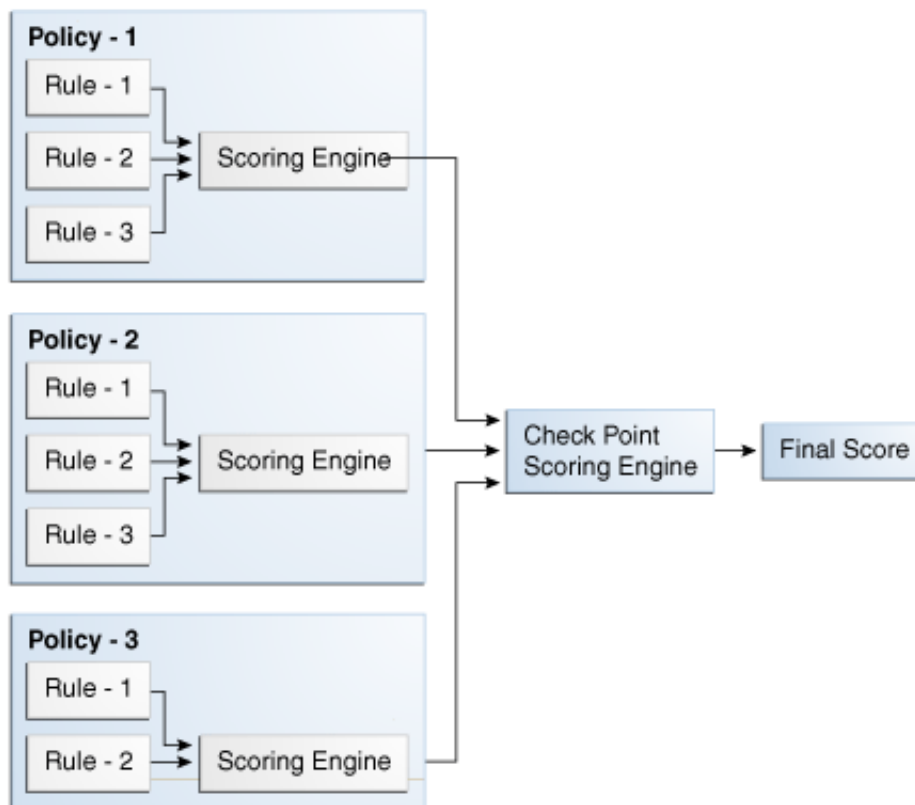
The checkpoint score is determined by applying the policy set scoring engine to the score result of the policies underneath the checkpoint.

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 12-1 Scoring



12.2.1 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 12–2 Score Propagation

The screenshot displays a risk scoring interface with the following sections:

- Sessions:** 4005
- Session Details:** Request ID 52_7f37031a9088c280a66b330bafc3b..., Application ID bharosaUIOGrp, Session ID 4005, Location Private, Private, Private, Device Score 0.
- Login Details:** (Collapsed)
- Checkpoints (5) / Transactions (0):** Expand All, Collapse All, Default View.
- Device Identification:** Risk Score 0, 1 milliseconds.
- Pre-Authentication:** Risk Score 0, Allow, 87 milliseconds.
- Policies (8):** (Collapsed)
- Post-Authentication:** Risk Score 1000, ChallengeQuestionPad, 24 milliseconds.
- Actions (1):** ChallengeQuestionPad (Final Action: Yes).
- Policies (6):** View, Launch Policy Explorer.

Name	Status	Scoring Engine	Time	Weight	Score
readPolicyPhilo1	Executed	Average	0	100	1000
Challenge user - roopang	Executed	Average	0	100	1000
Challenge user	Triggered		0	100	1000
ChallengeQuestionPad					
KBA Registration Check	Executed	Average	0	100	0

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 propagated from the rules level to the final level.

12.2.2 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.

12.2.3 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.

12.2.4 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.

12.3 Score Calculations

12.3.1 Policy Score

12.3.1.1 Aggregate Score

Sum of the scores of all triggered rules divided by count of rules.

12.3.1.2 Average Score

Sum of the scores of all triggered rules divided by count of triggered rules

12.3.1.3 Maximum Score

Higher score out of all triggered rules

12.3.1.4 Minimum Score

Lower score out of all triggered rules

12.3.1.5 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

12.3.1.6 Weighted Maximum Score

larger score (S * weight modifier specified by the policy) out of all triggered rules

12.3.1.7 Weighted Minimum Score

lower score (S * weight modifier specified by the policy) out of all triggered rules

12.3.2 Checkpoint Score

12.3.2.1 Average Score

Sum of the scores of all policies within the checkpoint divided by the count of all policies

12.3.2.2 Maximum Score

Higher score out of all policies

12.3.2.3 Minimum Score

Lower score out of all policies

12.3.2.4 Weighted Average Score

sum of policies ($S \times$ weight multiplier specified by the policy set) within the checkpoint divided by count of all policies

12.3.2.5 Weighted Maximum Score

larger score out of all policies ($s \times$ weight multiplier specified by the policy set)

12.3.2.6 Weighted Minimum Score

lower score out of all policies ($s \times$ weight multiplier specified by the policy set)

12.4 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 look at 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 will be ignored when scores are aggregated.

Managing System Snapshots

This chapter describes the Universal Risk Snapshot feature, which is new in Oracle Adaptive Access Manager 11g.

13.1 Concepts

This section introduces you to the concept of snapshots and how they are used in Oracle Adaptive Access Manager.

Using Universal Risk Snapshot, 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.

13.1.1 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

13.1.2 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.

13.1.3 Snapshot Metadata

For snapshots, the metadata that will be 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)	

13.1.4 Backup

A backup saves all the existing configurations (both active and inactive items) including all group definitions. Only Action and Alert group members will be 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.

13.1.5 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 will 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.

13.1.6 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 will contain members.

13.2 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. Double-click **System Snapshot** under **Environment** in the Navigation tree.

Alternative methods to open search pages are listed in [Section 3.9, "Access to Search, Create, and Import."](#)

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

13.3 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, select **System Snapshots**. The **System Snapshots Search** page is displayed.
2. Specify criteria in the Search Filter to locate the snapshot and click **Search**.

- The search is not case-sensitive.
- The search is a "contains" search. Results will be returned if you enter part of the name in the search.
- The search trims 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 13–1 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 locate 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.

13.4 Viewing Details of a Snapshot

To view details for a snapshot:

1. In the Navigation tree, select **System Snapshots**. 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 and notes 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

13.5 Creating a Backup

To create a backup:

1. In the Navigation tree, select **System Snapshots**. 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

13.5.1 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.

13.5.2 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.

13.5.3 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.

13.6 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.

13.6.1 Steps to Restore Selected Snapshot

To perform the restore operation:

1. In the Navigation tree, select **System Snapshots**. 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 will appear if the file was in the wrong format.

13.6.2 Loading and Restoring a Snapshot

Select a snapshot file, and click the **Load** button to load the snapshot into the system database.

If you press **Load**, the loaded snapshot is restored and becomes the current snapshot. If you select this option, you will not be able to preview the snapshot before restoring it.

13.6.3 Snapshot Restore Considerations

Snapshot restore considerations are described in this section.

13.6.3.1 Snapshot in Live System (Single Server)

Snapshot ZIP files will have server version from which it was taken. When re-storing if the version is determined to be in-compatible then the snapshot restore will fail.

If the snapshot is restored in a system that is running, the effect will be applicable in about 30 seconds when all the database artifacts are reloaded.

13.6.3.2 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 will be 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.

13.6.3.3 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 will not function since it will be 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.

13.7 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**.

13.8 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

13.9 Diagnostics

All the logs related to snapshot creation and restoration are contained in the server log.

13.10 Use Cases

This section describes example use cases for using snapshots.

13.10.1 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 will alert Jeff to the files that will be overwritten.

13.10.2 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 will contain 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.

13.10.3 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.

13.10.4 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.

13.11 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 will not be broken when they are brought back into a system.

Part V

Autolearning

This part of the book contains instructions to configure the Autolearning features in Oracle Adaptive Access Manager.

It contains the following chapters:

- [Chapter 14, "Managing Autolearning"](#)
- [Chapter 15, "Managing Configurable Actions"](#)

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](#)
- [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](#)

14.1 Introduction and Concepts

This section introduces you to the concepts of autolearning and how they are used.

14.1.1 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.

14.1.2 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.

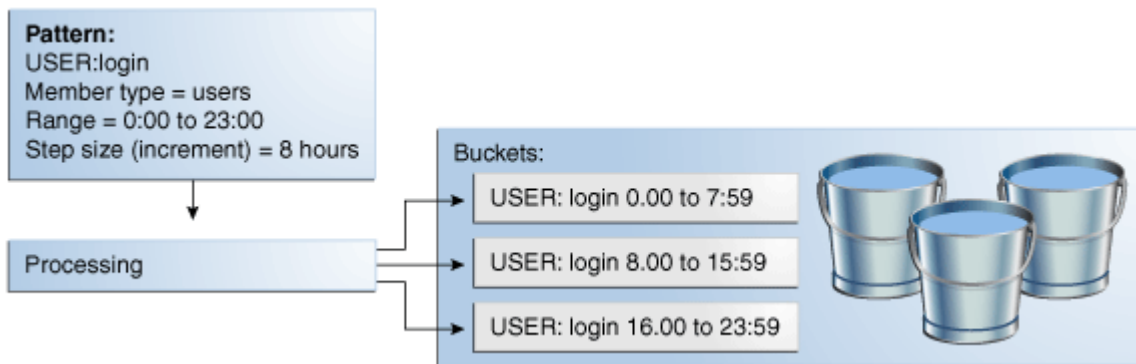
Patterns require that bucketing, member types, and attributes to be defined. As well, rules must be configured to harness the profiling conducted by the patterns.

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 14–1 shows a bucket creation and population example.

Figure 14–1 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 will automatically keep from overlapping with each other based on the other buckets already in the system. As shown in Figure 14–1, 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 will be incremented by one. If no user has ever logged into this system between 7:00 and 14:59 then Oracle Adaptive Access Manager will also create that bucket as part of the processing. This 7:00 and 14:59 bucket then would be used to record login time behavior for all users going forward.

After creation, the buckets will be populated with the logins of users that have fallen within each 8-hour time range.

Oracle Adaptive Access Manager will only record 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 will be saved in each user profile.

14.1.3 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 will collect 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 will be 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 will be more flexible and manageable in the long run.

14.1.4 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**

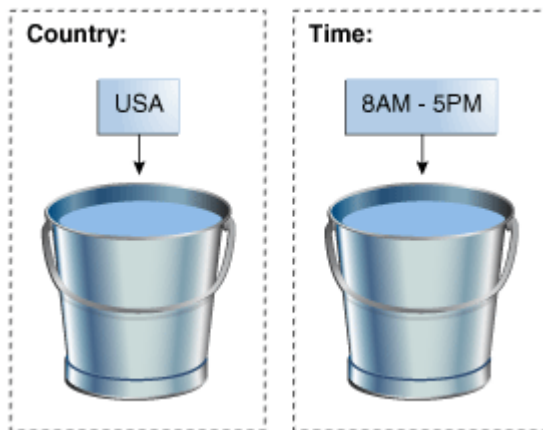
Single-bucket patterns create and populate one bucket with the exact data points and value ranges specified in the pattern.

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 14–2 Single Bucket



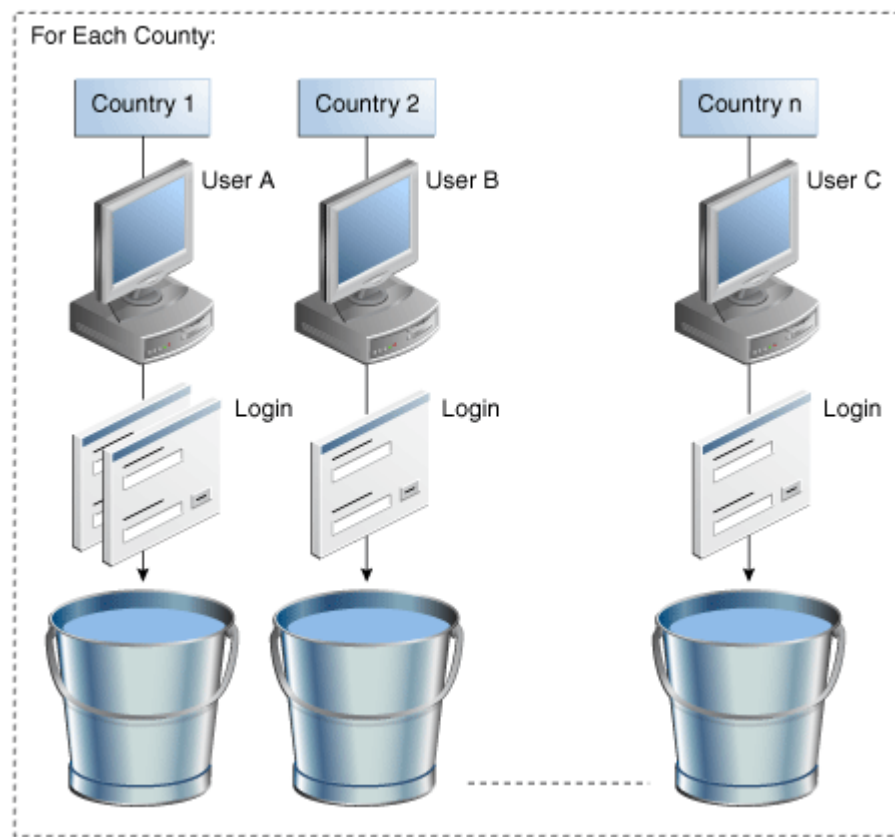
- **Multi-Bucket**

Multi-bucket patterns usually create more buckets than single-bucket patterns. They create buckets as required based on the parameter configurations.

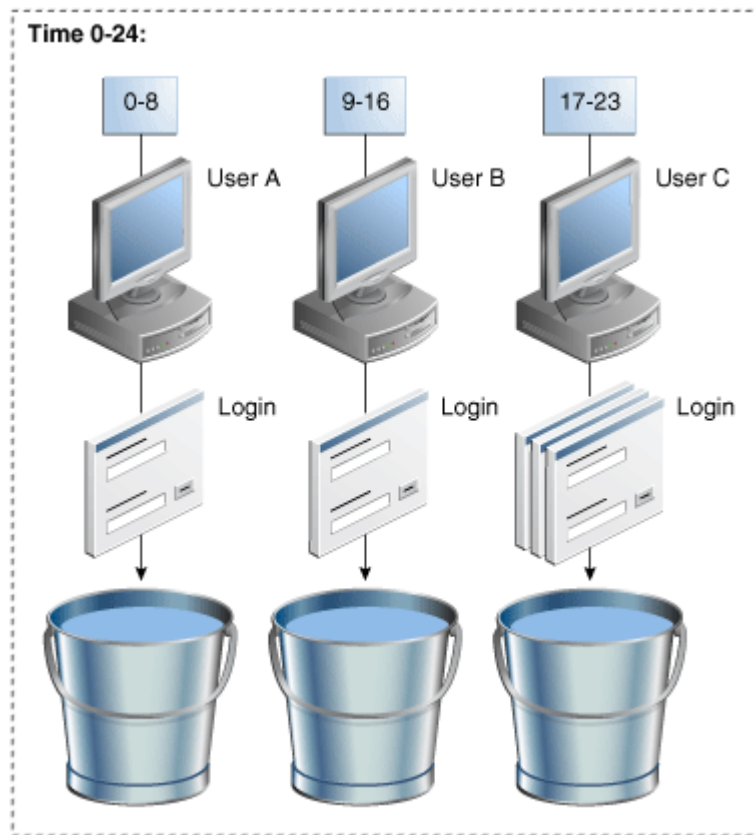
You configure the data types and samples you want Oracle Adaptive Access Manager to generate buckets from, and then during pattern processing Oracle Adaptive Access Manager creates buckets as needed to capture behaviors.

For example:

- If you specify "For each" as the compare operator and country as the attribute, Oracle Adaptive Access Manager will create 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 will create a Canada bucket and add that user as a member with a count of one. The next user to log in from Canada will be 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 will be incremented.

Figure 14-3 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 will be created, one for each 8-hour time slot in which logins occur.

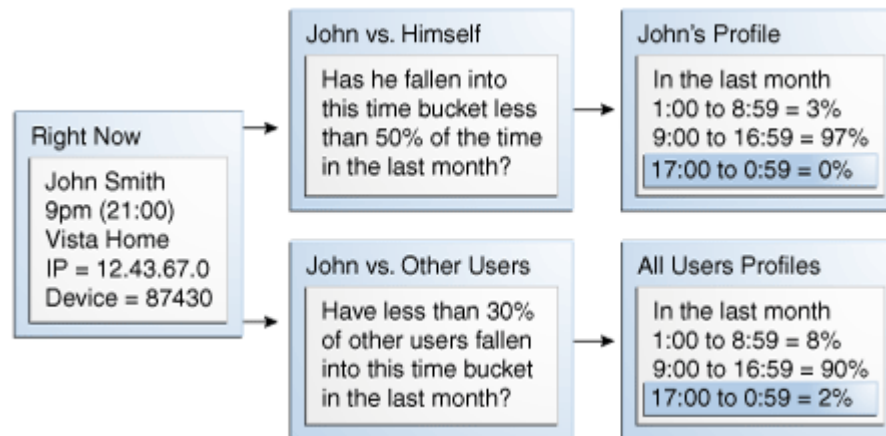
Figure 14-4 Time Multi-Buckets

14.1.5 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 look at 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.

Figure 14-5 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)
If User A logs in at 18:07 using Device X from IP Y	medium - high risk (device in #4)

Scenarios	Risk
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's important to emphasize that each of these elements is evaluated for membership in the time profiles independently in this example.

14.1.6 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 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.

14.2 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 14.3.1, "Importing Basic Authentication-Related Entities."](#)
2. Enable autolearning properties.
See [Section 14.3.2, "Enabling Autolearning Properties."](#)
3. Create patterns.

Define patterns, add attributes, and activate /enable the patterns so that the system can start collecting pattern data.

See [Section 14.9, "Creating and Editing Patterns."](#)

4. Finally, use the patterns in rule evaluation.

For information on using autolearning, see [Section 14.12, "Using Autolearning Data/Profiling Data."](#)

To verify that autolearning is turned on and working, see [Chapter 25, "Troubleshooting."](#)

14.3 Before You Begin

Before using the Autolearning feature, read through [Section 14.1, "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.

14.3.1 Importing Basic Authentication-Related Entities

The actors that are tracked during authentication are called authentication entities and include user, city, device, and so on. These basic entities are required to enable conditions that are used for patterns. Before you begin using the Autolearning feature, you must import these basic entities into your system. Basic required entities are shipped along with Oracle Adaptive Access Manager in the `Auth_EntityDefinition.zip` file, which is located in the `oaam_init` directory.

To import the entities:

1. Navigate to the **Entities Search** page, as described in [Section 16.2, "Navigating to the Entities Search Page."](#)
2. Click **Import Entities**.
3. In the **Import Pattern** screen, 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.

14.3.2 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 for the transaction-related patterns to work. Transaction related patterns are the one that process the transaction related data for autolearning. An example is a pattern that profiles users who are performing wire transfer operations.

14.3.3 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" will trigger 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 A, "Pattern Processing."](#)

14.4 User Flows

User flows are presented for:

- [Creating a New Pattern](#)
- [Editing a Pattern](#)

14.4.1 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 will be created successfully.

14.4.2 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 will be edited successfully.

14.5 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, "Access to 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

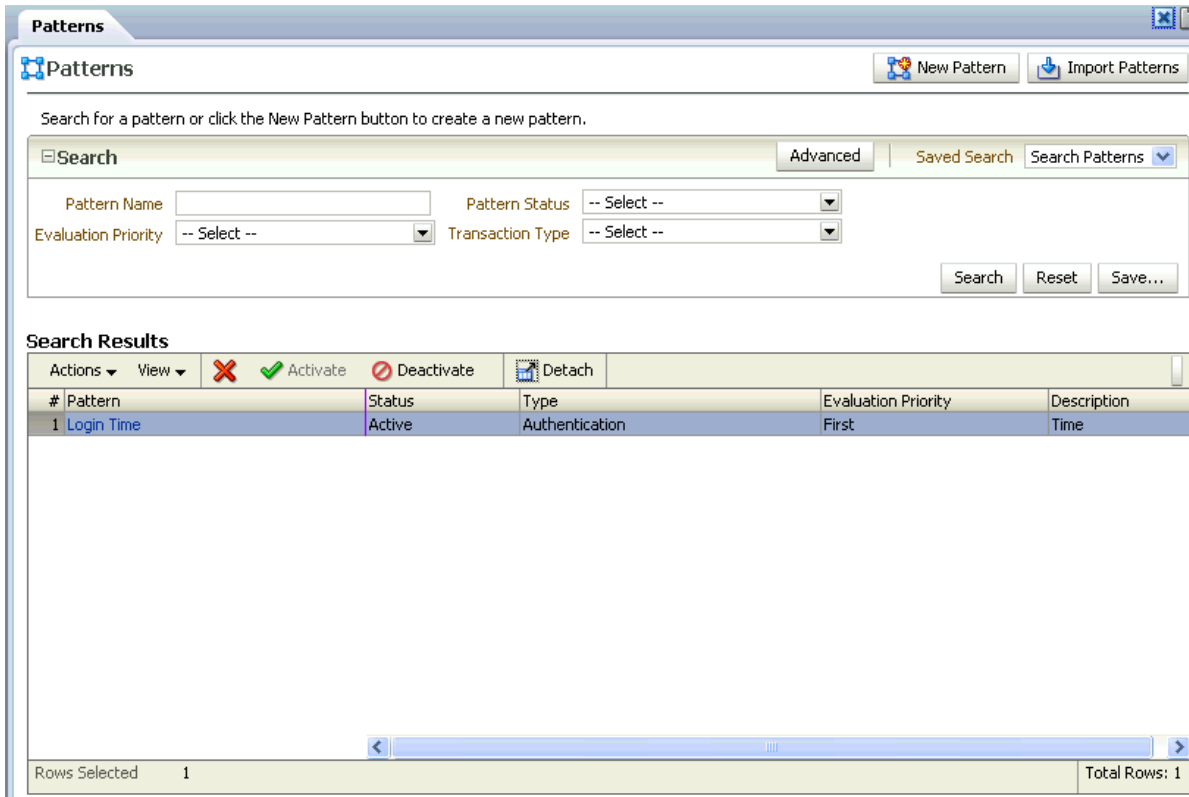
14.6 Searching for a Pattern

To search for a Pattern:

1. Navigate to the **Patterns Search** page, as described in [Section 14.5, "Navigating to the Patterns Search Page."](#)

An example **Patterns Search** page is shown in [Figure 14–6](#).

Figure 14–6 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 14–1](#).

If you want to reset the search parameters to the default setting, use the **Reset** button.

Table 14–1 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	<p>The priority in which the collected data is evaluated.</p> <ul style="list-style-type: none"> ■ 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.
Pattern Status	<p>The state of the pattern. These are the pattern states:</p> <ul style="list-style-type: none"> ■ Active If data must be collected, the pattern must be in the active state. ■ Inactive If the pattern definition 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 If there is a problem with the pattern, you can mark the pattern as invalid to signal other operators. No autolearning data analysis will performed for a pattern in this state. ■ Deleted The pattern has been deleted, but system must keep this record to maintain data integrity. No autolearning data analysis will be performed for pattern in this state. It is recommended that you do not use the Deleted status. This status may not be available in future releases.
Transaction Type	<p>The Transaction Definitions that have been configured in this specific Oracle Adaptive Access Manager installation.</p> <p>The type of process such as authentication (login), bill pay, wire transfer, address change, and so on that autolearning is profiling entities for.</p>
Creation Method	<p>The type of bucket the Pattern had been created as.</p> <ul style="list-style-type: none"> ■ Single Bucket - Single-bucket patterns will create and populate one bucket with the exact data points and value ranges specified in the pattern ■ Multi- Bucket – Multi-bucket patterns have buckets for sub-ranges of a parameter range

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.

14.7 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 14.5, "Navigating to the Patterns Search Page."](#)
2. Search for the pattern of interest, by following the instructions in [Section 14.6, "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.

14.8 Viewing Pattern Details

This section provides details on viewing patterns.

14.8.1 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 14.7, "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).

14.9 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](#)

14.9.1 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 14.5, "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, "Access to 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 transaction type is **Authentication**.
Other transaction types shown are the transaction definitions that have been set up in your system.
Only active transaction types are available in the list.
Examples of transaction types are authentication, bill pay, money transfer, merchant purchase, credit card, and others. For example, if you select merchant purchase as the transaction type, you want to gather data on the activity of all the members during merchant purchases.
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.

Member type list values depend on the transaction type selected.

If the **Transaction Type** selected is **Authentication**, member types available are **User, City, State, Country**, and others.

If, the **Transaction Type** selected is any transaction from the database, for example, Retail Commerce, Internet, Bill Pay, the member types available are data elements for that transaction. For example, if the **Transaction Type** is Internet Banking, the member type data elements could be customer and bank name.

One or more member types can be selected for a pattern
 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 14–7 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.

For information, see [Section 14.9.2, "Adding Attributes."](#)

For information on attributes, see [Section 14.1.3, "Member Types and Attributes."](#)

11. Activate the pattern.

To activate the pattern, see [Section 14.9.3.1, "Activating Patterns."](#)

To use the patterns in rule evaluation, see [Section 14.12, "Using Autolearning Data/Profiling Data."](#)

To verify that autolearning is working, see [Chapter 25, "Troubleshooting."](#)

14.9.2 Adding Attributes

For information on attributes, see [Section 14.1.3, "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 14.8.1, "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** screen, 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 we 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 14.14, "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.

14.9.3 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.

14.9.3.1 Activating Patterns

To activate patterns:

1. Navigate to the **Patterns Search** page, as described in [Section 14.5, "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 14.6, "Searching for a Pattern."](#)
3. Select the row for each pattern you want to activate.
4. Press the **Activate** button.

14.9.3.2 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.

14.9.4 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 14.7, "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 14.9.5, "Changing the Status of the Pattern."](#)
4. Add or change the member types.
For information, see [Section 14.9.6, "Adding or Changing Member Types."](#)
For information about member types, see [Section 14.1.3, "Member Types and Attributes."](#)
5. Change the evaluation priority

To change the evaluation priority, see [Section 14.9.7, "Changing the Evaluation Priority."](#)

6. To add attributes, see [Section 14.9.2, "Adding Attributes."](#)

For information on attributes, see [Section 14.1.3, "Member Types and Attributes."](#)

7. To edit attributes, see [Section 14.9.8, "Editing Attributes."](#)

8. To delete attributes, see [Section 14.9.9, "Deleting Attributes."](#)

9. Click **Apply**.

14.9.5 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 will be performed for 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.

14.9.6 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 14.1.3, "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 14.7, "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.

14.9.7 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 14.7, "Navigating to the Patterns Details Page."](#)
2. In the **Summary** tab, change the evaluation priority.

14.9.8 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 14.8.1, "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**.

14.9.9 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 14.8.1, "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**.

14.10 Importing and Exporting Patterns

You may want to import and export patterns from other applications. This section explains how to import and export patterns.

14.10.1 Importing Patterns

To import patterns:

1. Navigate to the **Patterns Search** page, as described in [Section 14.5, "Navigating to the Patterns Search Page."](#)

2. In the **Patterns Search** page, click **Import Pattern**.
3. In the **Pattern Import** screen, click **Browse** and locate the pattern file you want to import.
4. Click **OK**.

14.10.2 Exporting Patterns

To export patterns:

1. Navigate to the **Patterns Search** page, as described in [Section 14.5, "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 14.6, "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** screen, click **Export**.
6. In the **Save** screen, click **OK**.

14.11 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 14.5, "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 14.6, "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.

14.12 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.

14.12.1 Create a Policy that Uses Autolearning Conditions

Create a policy that will use the autolearning conditions.

For instructions to create a policy, see [Section 14.13.1, "Use Case: Challenge Users If Log In Different Time Than Normally."](#)

14.12.2 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 14.13.4, "Use Case: User Logs in During a Certain Time of Day More Than X Times."](#)

The rule will evaluate the pattern you selected and autolearning processing will be performed.

To learn more about autolearning conditions, see [Appendix B, "Conditions Reference."](#)

14.12.3 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 14.13.2, "Use Case: Test a Pattern."](#)

14.13 Use Cases

This section describes example use cases for autolearning and patterns.

14.13.1 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.

14.13.2 Use Case: Test a Pattern

Jeff a Security Administrator must make sure the pattern he configured in his use (see [Section 14.13.1, "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.

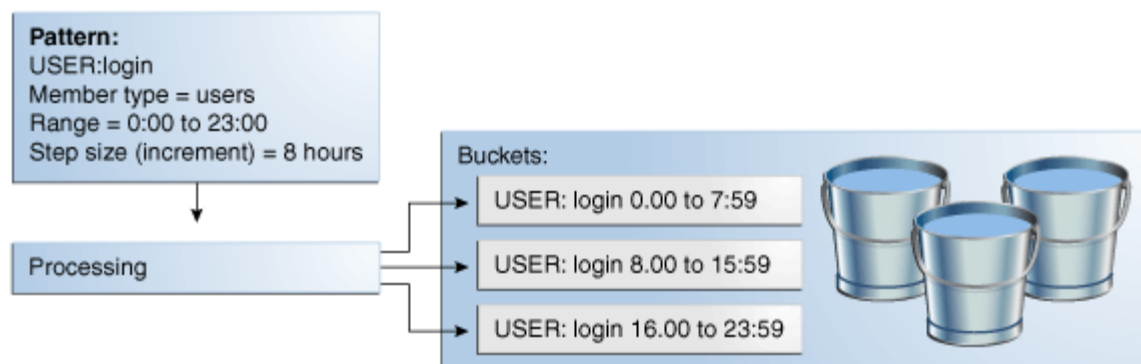
In this way Jeff can see the session where the alert was triggered was at a time that fell into a bucket it had not previously fallen into more than 5% of the time in the last month. From that, Jeff confirms that the policy configuration and pattern are functioning as designed.

14.13.3 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 14–8 Using Buckets to Track Off-Hour Access



1. Navigate to the **Patterns Search** page, as described in [Section 14.5, "Navigating to the Patterns Search Page."](#)
2. In the **Patterns Search** page, click the **New Pattern** button.
3. In the **Create Pattern** screen, 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.
12. In the **Attributes** page, click the **Add** button.
13. In the **Add Attributes** screen, 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.

14.13.4 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 10, "Managing Groups."](#)

4. Create a policy that will use 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.

14.13.5 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 B.1.2.2, "Entity: Entity is member of pattern less than some percent times."](#)

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.

14.13.6 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 we 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).

14.13.7 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 ["Entity: Entity is member of pattern less than some percent times"](#).

- 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.

14.13.8 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.

14.13.9 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
 - **Evaluation Priority:** High
 - **Description:** Pattern to track the state usage and frequencyClick **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 displayed.
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 [Entity: 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.

14.14 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.

14.14.1 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.

14.14.2 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.

14.14.3 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.

14.14.4 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).

14.14.5 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.

14.14.6 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.

14.14.7 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).

14.14.8 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).

14.14.9 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.

14.14.10 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.

14.14.11 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.

14.14.12 Range

Range is usually used with numerics.

Figure 14–9 Range Compare Operator

The screenshot shows a dialog box titled "Add Attribute" with a close button in the top right corner. Below the title bar, there is a instruction: "Specify the condition information for the attribute instance and click the Apply button." The dialog contains several fields:

- Label Time**: A text field containing "Time when the user is logged in".
- Definition**: A text field containing "Time when the user is logged in".
- Status**: A text field containing "Active".
- Description**: A large empty text area.
- * Compare Operator**: A dropdown menu currently set to "Range".
- * Start Value**: A numeric input field containing "0".
- End Value**: An empty numeric input field.
- Increment Step**: A numeric input field containing "0".

At the bottom right of the dialog, there are four buttons: "Back", "Next", "Add", and "Cancel".

14.14.12.1 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).

14.14.12.2 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).

14.14.12.3 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.

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**.

15.1 Introduction and Concepts

This section introduces you to the concept of configurable actions and how they are used in Oracle Adaptive Access Manager.

15.1.1 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 15.20, "Out-of-the-Box Configurable Actions."](#)

15.1.2 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:

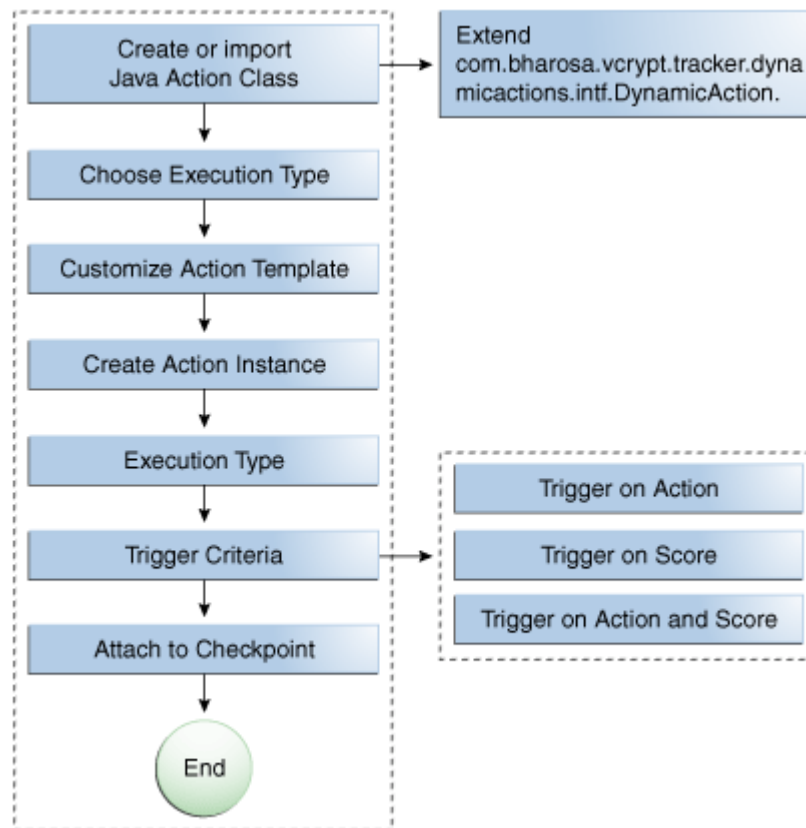
- Add user to a white-list group
- Add user to black-list group
- Add IP to IP white-list group
- Add IP to IP black-list group

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."

15.1.3 Deploying a Configurable Action

A flow chart illustrating the deployment of a Configuration Action is shown in [Figure 15-1](#).

Figure 15-1 *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 can be imported from `MW_HOME/IDM_ORACLE_HOME/oaam/init/OOTB_Configurable_Actions.zip` file

If the out-of-the-box configurable action templates are not available in the system, import them.

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.

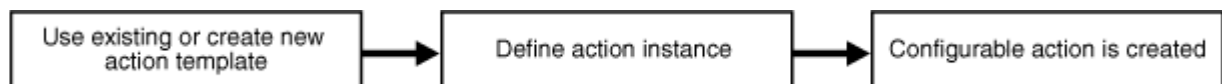
15.2 Creating Configurable Actions

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 15–2 Configurable Action wizard Flow



15.2.1 Define New Action Template

If you want to define a new action template, see [Section 15.6, "Creating a New Action Template"](#) for detailed information.

15.2.2 Use Existing Action Template

If you want to use an existing action template, see [Section 15.4, "Searching for Action Templates."](#)

15.2.3 Create Action Instance

To define an action instance, see [Section 15.9, "Creating an Action Instance and Adding it to a Checkpoint"](#) for detailed information.

15.3 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, "Access to Search, Create, and Import."](#)

15.4 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 15.3, "Navigating to the Action Templates Search Page."](#)

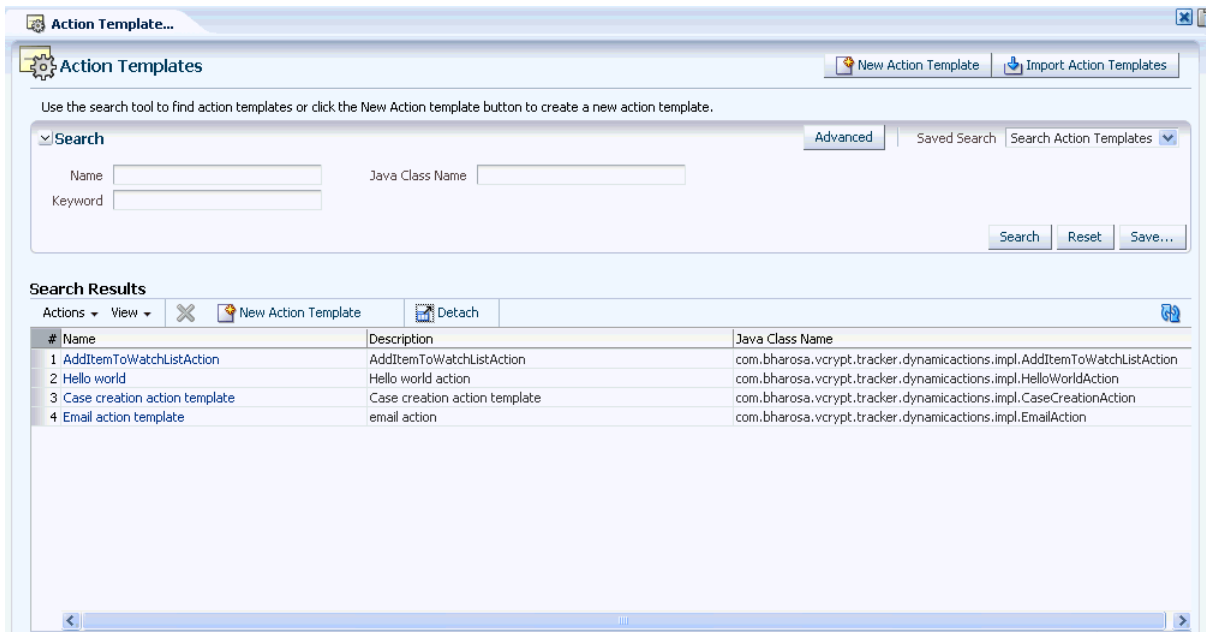
The **Search Results** table will display no results when the **Action Templates Search** page first appears.

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.

An example **Action Templates Search** page is shown in [Figure 15–3](#).

Figure 15–3 Action Templates Search page



The action templates displayed are those that match the criteria specified in the Name, Java Class Name, and Keyword fields ([Table 15-1](#)).

Table 15-1 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.

15.5 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 15.4, "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.

15.6 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 15.3, "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, "Access to 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.

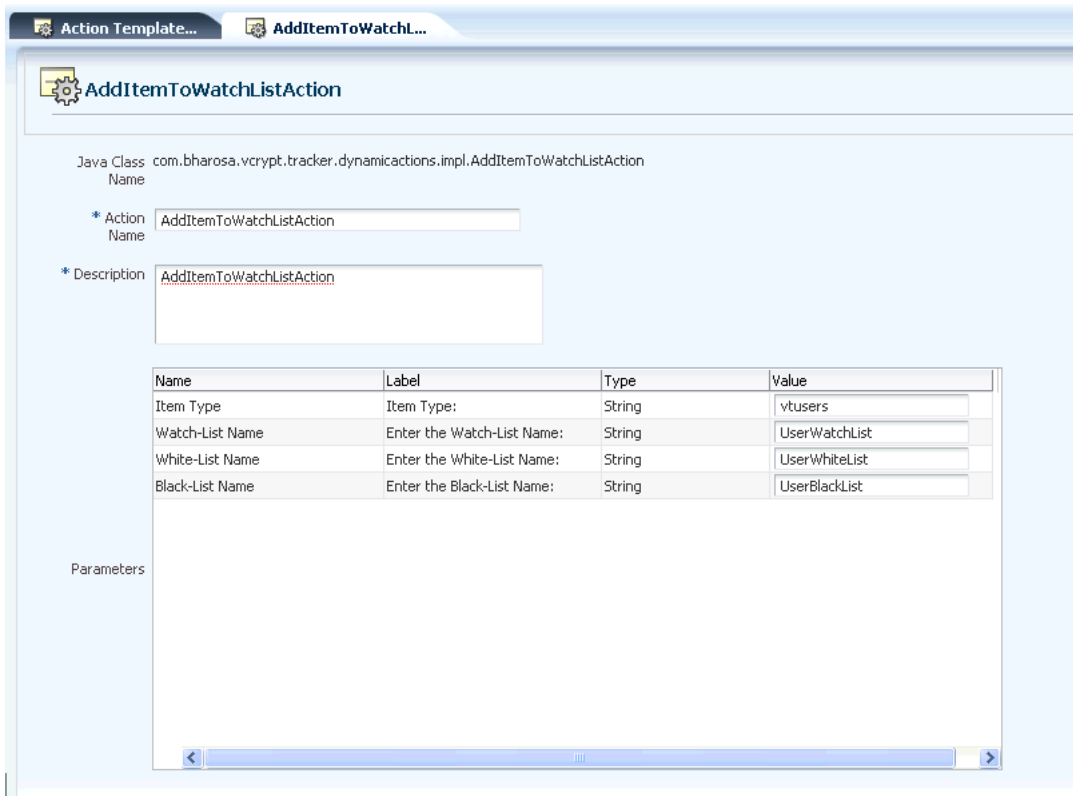
Name	Label	Type	Value
Item Type	Item Type:	String	<value>
Watch-List Name	Enter the Watch-List Name:	String	<value>
White-List Name	Enter the White-List Name:	String	<value>
Black-List Name	Enter the Black-List Name:	String	<value>

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.

Figure 15–4 Creating Action Template



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 15.9, "Creating an Action Instance and Adding it to a Checkpoint."](#)

15.7 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, "Access to Search, Create, and Import."](#)

15.8 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 15.7, "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 15-2](#)).

Table 15-2 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	<p>There are two execution types: Synchronous and Asynchronous</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <ul style="list-style-type: none"> ■ 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.

15.9 Creating an Action Instance and Adding it to a Checkpoint

To create an action instance, follow the procedure in this section.

[Figure 15-5](#) shows an example of an action instance.

Figure 15–5 Action Instance

Name	Label	Type	Value
Item Type	Item Type:	String	vtusers
Watch-List Name	Enter the Watch-List	String	AmtTransferSuspectedList
White-List Name	Enter the White-List	String	UserWhiteList

Create Action Instance and Associate it to a Checkpoint

1. Navigate to the **Action Instance Search** page, as described in [Section 15.7, "Navigating to the Action Instances Search Page."](#)

2. Click **New Action Instance**.

Alternative methods to open create pages are listed in [Section 3.9, "Access to 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** screen, 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.

15.10 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.

15.11 Editing an Action Template

To edit details about a specific action template:

1. Search for the action template, as described in [Section 15.4, "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.

15.12 Exporting Action Templates

To export action templates:

1. Search for the action template, as described in [Section 15.4, "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** screen, click **Export**.
5. In the **Save** screen, click **OK**.

15.13 Importing Action Templates

To import action templates:

1. Navigate to the **Action Templates Search** page, as described in [Section 15.3, "Navigating to the Action Templates Search Page."](#)
2. In the **Action Templates Search** page, click **Import**.
3. In the **Action Templates Import** screen, click **Browse** and locate the action templates file you want to import.
4. Click **OK**.

15.14 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 15.12, "Exporting Action Templates."](#)
2. Import the action template into the target system. Refer to [Section 15.13, "Importing Action Templates."](#)
3. If the configurable action is a customized one, skip Steps 1 and 2. Use the Oracle Adaptive Access Manager 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 11g, do not copy the custom jars to OAAM webapp folders.

Migrating 10g Action Templates to 11g

In the 11g user interface for Action Templates, the Notes field has been removed. If the Notes field contains text in the 10g Action Templates, after migration to 11g, these notes will be appended (combined) with the description text.

15.15 Deleting Action Templates

To delete action templates:

1. Search for the action template, as described in [Section 15.4, "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.

15.16 Viewing a List of Configurable Action Instances

1. Navigate to the Action Instances Search page, as described in [Section 15.7, "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.

15.17 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 15.7, "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.

15.18 Editing an Action Instance

To edit an action instance:

1. Navigate to the **Action Instance Search** page, as described in [Section 15.7, "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.

15.19 Deleting an Existing Action Instance

To delete an action instance:

1. Navigate to the **Action Instances Search** page, as described in [Section 15.7, "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.

15.20 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 from the oaam_init directory.

15.20.1 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 15.3, "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.

15.20.2 Defining AddItemToListAction

To define AddItemToListAction:

1. Navigate to the **Action Templates Search** page, as described in [Section 15.3, "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.

15.21 Use Cases

This section describes example use cases for configurable actions

15.21.1 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.

15.21.2 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**.

15.21.3 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 11g, he does this by adding his custom jars to the Oracle Adaptive Access Manager 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.interfaces.DynamicAction`
 java interface.
2. He can compile his class by linking the Oracle Adaptive Access Manager jars from `$IDM_ORACLE_HOME\oaam\native\java\lib` folder.
3. He should then test his custom configurable action to make sure it is working correctly.
4. He should then package his class as a jar file and create shared library by the following the structure of Oracle Adaptive Access Manager Extensions shared library that is available in `$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 Oracle Adaptive Access Manager extensions library using his shared library and then import his custom configurable action template from his export file.

15.21.4 Use Case: Create Case

Matt is a Security Administrator. He needs to configurable an 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.

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 16, "Creating and Managing Entities"](#)
- [Chapter 17, "Managing Transactions"](#)

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.

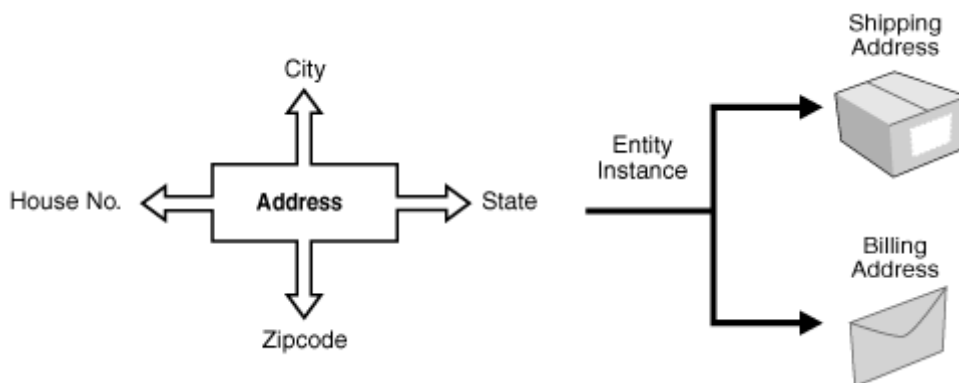
16.1 Introduction and Concepts

This section introduces you to the concept of entities.

16.1.1 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 16–1 Address Entity



16.1.2 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.

16.1.3 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.

16.1.4 ID Scheme

An ID scheme consists of the data elements that can uniquely identify an entity, in other words, we 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.

16.1.5 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.

16.1.6 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.

16.2 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.

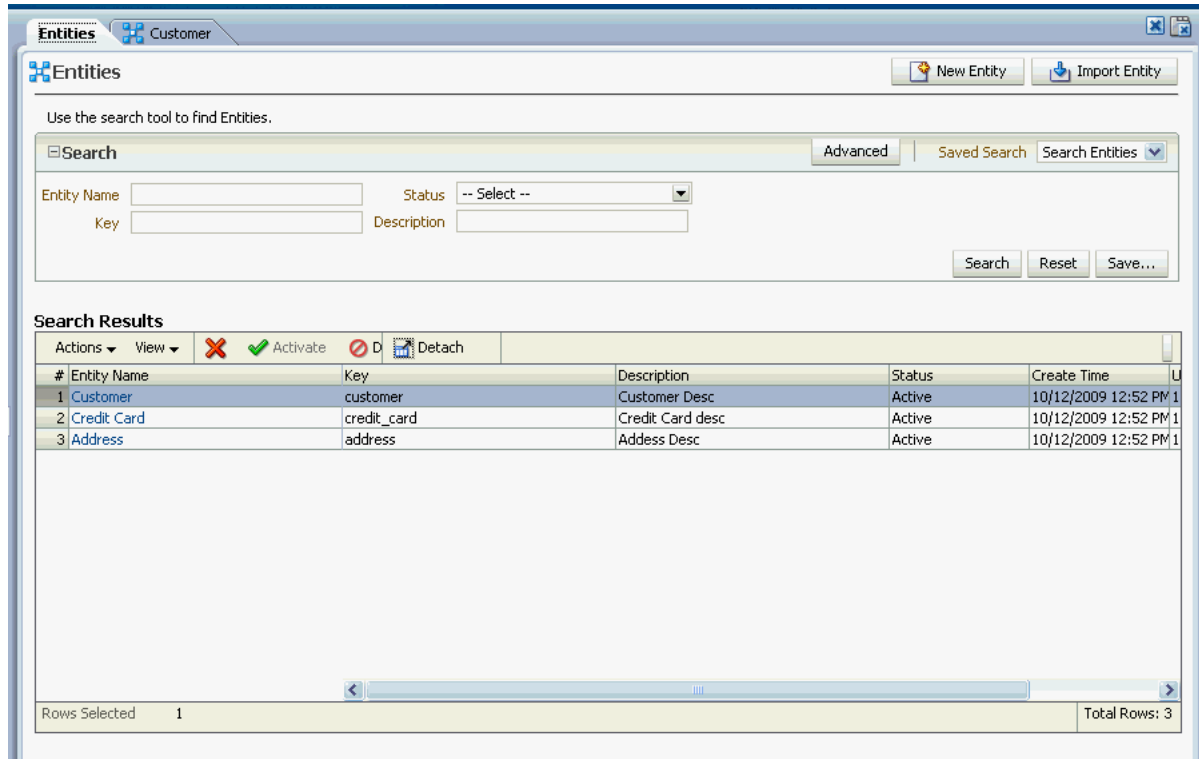
The Entities Search page is the starting place for managing entities. From the Entities Search page, you can:

- 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 16–2](#).

Figure 16–2 Entities Search page



16.3 Searching for Entities

To search for entities:

1. Navigate to the **Entities Search** page, as described in [Section 16.2, "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 16–1](#).

Table 16–1 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.

16.4 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 16.9, "Activating Entities."](#)

16.4.1 Initial Steps

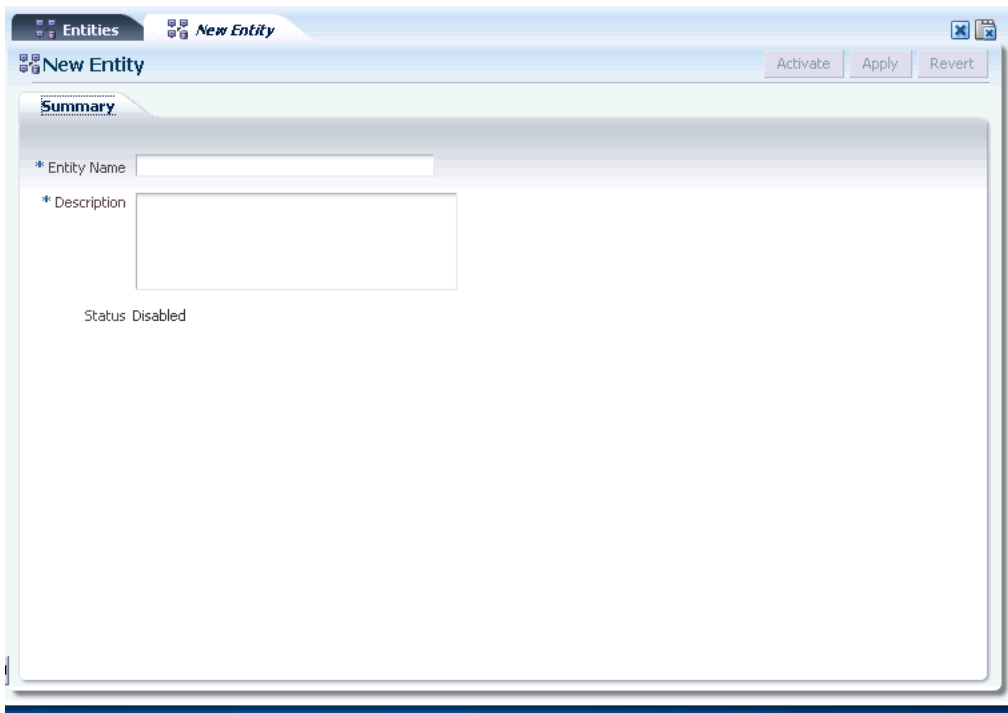
To create an entity, follow these steps.

1. Navigate to the **Entities Search** page, as described in [Section 16.2, "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, "Access to Search, Create, and Import."](#)

An example of a **New Entity** page is shown in [Figure 16–3](#).

Figure 16–3 *New Entity Page*



The screenshot shows a web browser window with the title 'Entities' and a sub-tab 'New Entity'. The main content area is titled 'New Entity' and has a 'Summary' tab selected. Below the tab, there are two text input fields: '* Entity Name' and '* Description'. The status is 'Status Disabled'. At the top right of the form area, there are three buttons: 'Activate', 'Apply', and 'Revert'.

3. In the **New Entity** page, enter the entity name.
The entity name must be unique.
4. Enter a description.
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.

16.4.2 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. Data 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 its **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.

16.4.3 Selecting Elements for the ID Scheme

In the **ID Scheme** tab, select the elements that you want to use to uniquely identify an entity.

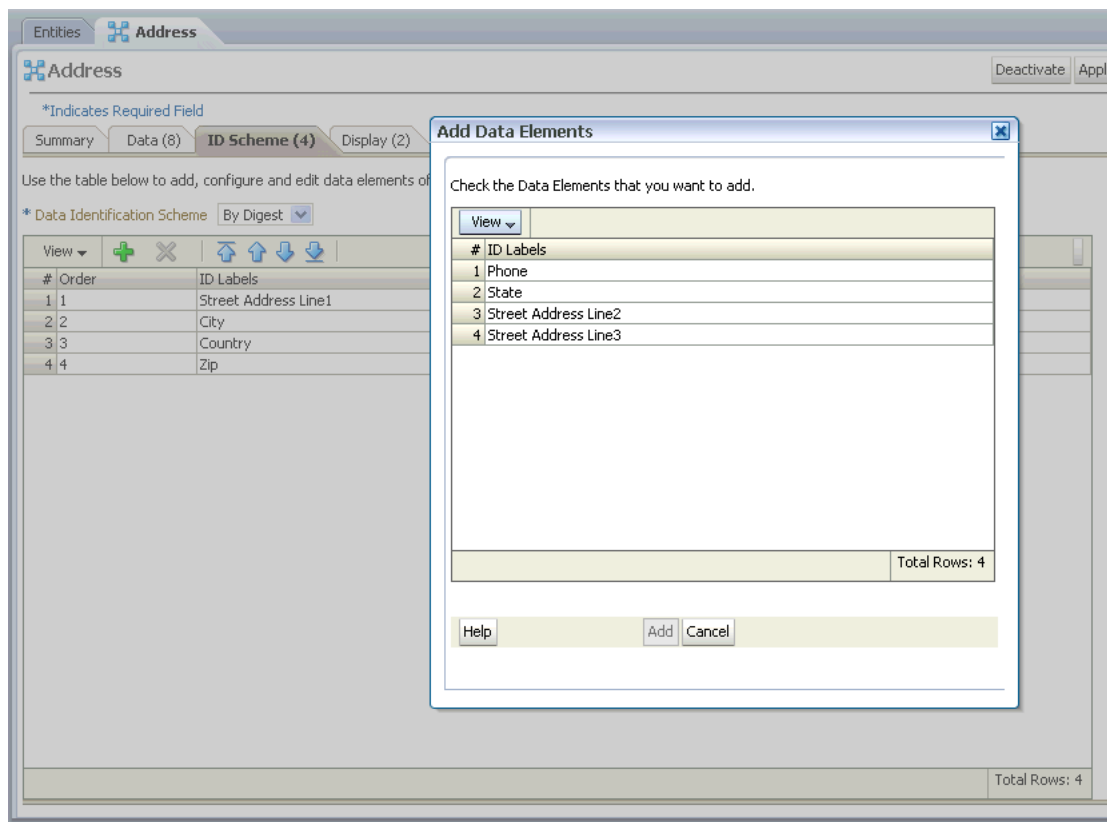
For example, the credit card entity has many attributes, but the way to uniquely identify a credit card is by using the 16-digit credit card number. In that case, the ID scheme is just the credit card number.

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 16-4](#).

Figure 16–4 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.

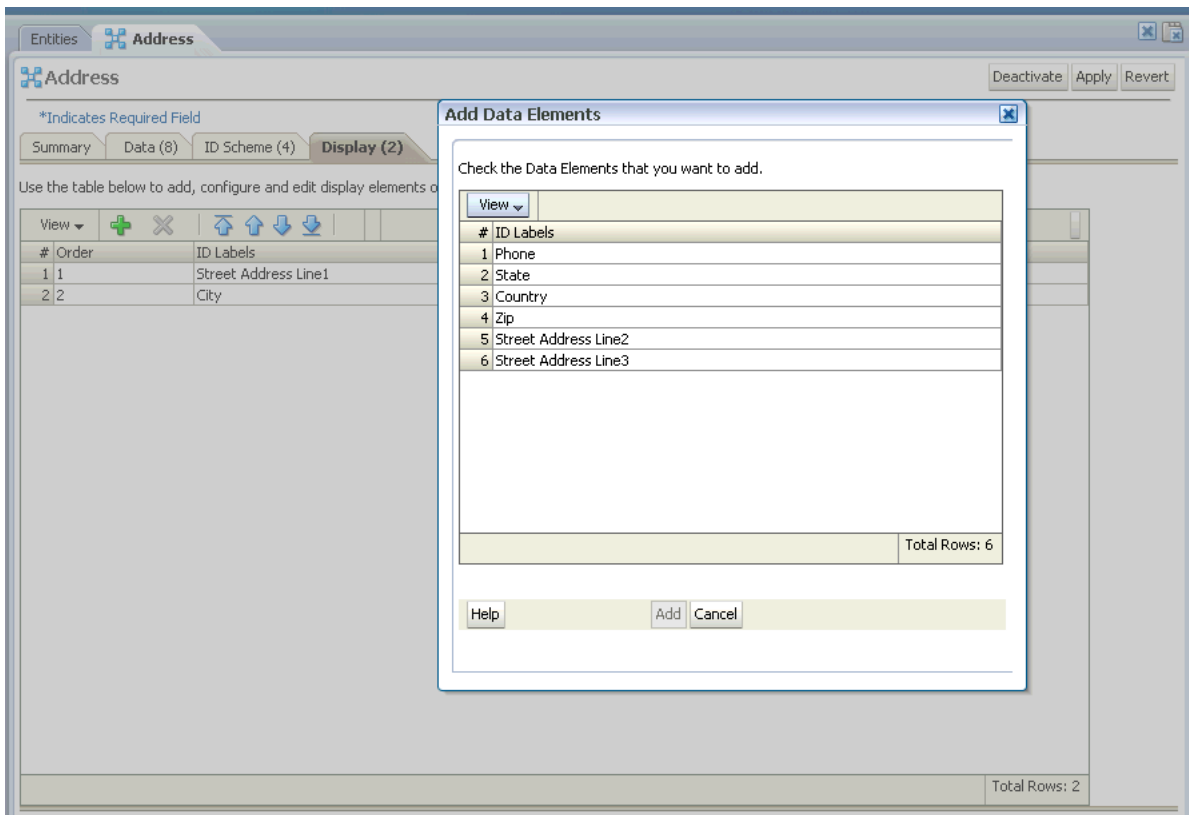
16.4.4 Specifying Data for the Display Scheme

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 16–5](#).

Figure 16–5 *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.

16.4.5 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 16.9, "Activating Entities."](#)

16.5 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 16.2, "Navigating to the Entities Search Page."](#)
2. From the **Entities Search** page, search for the entity you want.
The filters are described in [Table 16-1](#).
3. In the **Results** table, click the entity name.

An example of an **Entity Details** page is shown in [Figure 16-6](#).

Figure 16–6 Entity Details page

The screenshot shows a web application window titled 'Entities' with a sub-tab 'Credit Card'. The main content area is titled 'Credit Card' and contains several tabs: 'Summary', 'Data (3)', 'ID Scheme (2)', and 'Display (2)'. The 'Summary' tab is active and displays the following information:

- *Indicates Required Field
- * Entity Name: Credit Card (text input field)
- Key: credit_card
- * Description: Credit Card desc (text area)
- Status: Active
- Creation Date: 10/12/2009
- Last Updated: 10/12/2009

At the top right of the main content area, there are three buttons: 'Deactivate', 'Apply', and 'Revert'.

16.6 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 16.5, "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**.

16.7 Exporting Entities

To export entities:

1. Navigate to the **Entities Search** page, as described in [Section 16.2, "Navigating to the Entities Search Page."](#)
2. In the **Entities Search** page, enter the search criteria you want and click **Search**. Refer to [Section 16.3, "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**.

16.8 Importing Entities

To import entities:

1. Navigate to the **Entities Search** page, as described in [Section 16.2, "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**.

16.9 Activating Entities

To activate entities:

1. Navigate to the **Entities Search** page, as described in [Section 16.2, "Navigating to the Entities Search Page."](#)
2. In the **Entities Search** page, enter the search criteria you want and click **Search**. Refer to [Section 16.3, "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.

16.10 Deactivating Entities

To deactivate entities:

1. Navigate to the **Entities Search** page, as described in [Section 16.2, "Navigating to the Entities Search Page."](#)
2. In the **Entities Search** page, enter the search criteria you want and click **Search**. Refer to [Section 16.3, "Searching for Entities."](#)
3. Select the row for each entity you want to deactivate.
4. Press the **Deactivate** button.

16.11 Deleting Entities

To delete entities:

1. Navigate to the **Entities Search** page, as described in [Section 16.2, "Navigating to the Entities Search Page."](#)
2. In the **Entities Search** page, enter the search criteria you want and click **Search**. Refer to [Section 16.3, "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.

16.12 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.

16.13 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 it. 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.

Managing Transactions

This chapter focuses on the creation of transaction definitions. Information on other procedures will also be provided.

17.1 Introduction and Concepts

This section introduces you to the concept of transaction definitions and how they are used in Oracle Adaptive Access Manager.

17.1.1 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

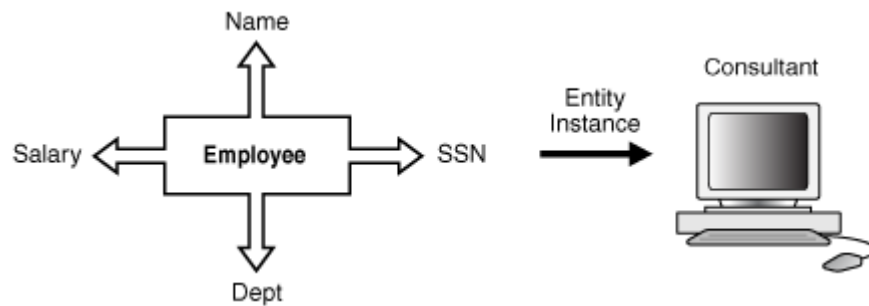
When defining a transaction at least one is mandatory.

17.1.2 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 17-1](#) shows an example of the employee entity.

Figure 17-1 Entity Example



17.1.3 Transaction Data

Transaction data is data that is considered:

- an abstract item
- data that does not have any attributes by itself
- data does not fit into any entity
- data that is unique by itself (standalone data)

Examples of transaction data is "Amount" and "Code."

17.1.4 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.

17.2 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:

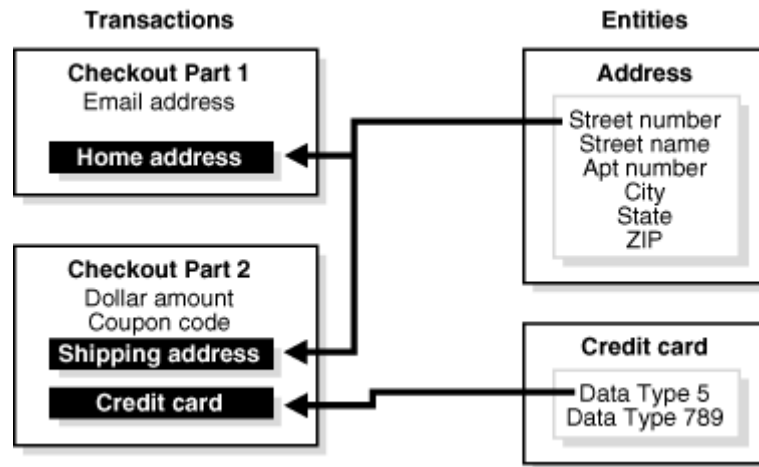
- Address
 - Account
 - Credit Card
 - Customer
 - Product Details
2. Create entities for objects in the real world and activate them.

For example, a home address entity can have StreetNumber, StreetName, AptNumber, City, State, and ZIP.

For details for creating entities refer to [Chapter 16, "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 17–2 Entities and Transaction Data Association with Source Data



4. Add the entities to the transaction definition.
Refer to [Section 17.8, "Adding an Existing Entity to the Transaction"](#) or [Section 17.9, "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 17.10, "Defining Transaction Data for the Transaction at the Oracle Adaptive Access Manager End"](#) for details.

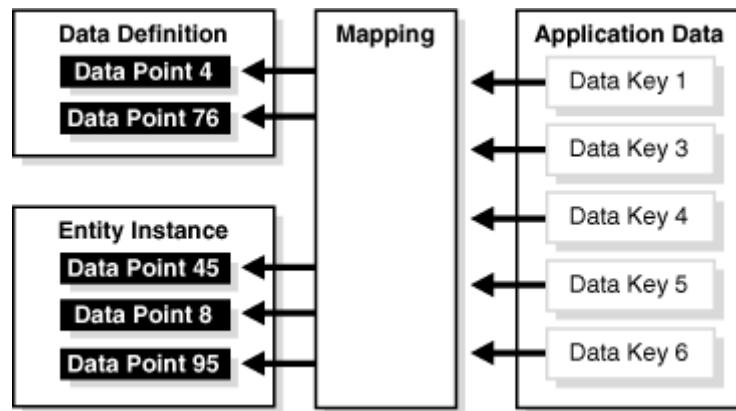
6. Define the parameters (source data elements) for the transaction from the client's end.

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 17.11, "Defining Parameters for the Transaction from the Client's End"](#) for details.

7. Map source data to transaction data and entities.
Refer to [Section 17.12.2, "Mapping Entities to the Source Data"](#) for details.
8. Activate the transaction definition.
Refer to [Section 17.17, "Activating a Transaction Definition"](#) for details.

Figure 17-3 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.

17.3 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.

17.4 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 17.4, "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 17–1, " Search Filter Criteria"](#).

If you want to reset the search parameters to the default setting, use the **Reset** button.

Table 17–1 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.

17.5 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.

17.6 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.

17.7 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.

17.8 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.

17.9 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 16.4.1, "Initial Steps"](#) in [Chapter 16, "Creating and Managing Entities"](#) for details.

3. In the **Entity Data** page, add data elements of the entity.

Refer to [Section 16.4.2, "Adding and Editing Data Elements"](#) in [Chapter 17, "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 16.4.3, "Selecting Elements for the ID Scheme"](#) in [Chapter 16, "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 16.4.4, "Specifying Data for the Display Scheme"](#) in [Chapter 16, "Creating and Managing Entities"](#) for details.

6. Perform Steps 1 through 5 to create new entities to add to the transaction definition.

17.10 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 DATA (for non-numeric), NUM_DATA (for numeric) columns in VT_TRX_DATA table in database.

Fields in **Entities** are mapped to DATA (for non-numeric), NUM_DATA (for numeric) columns in VT_ENTITY_ONE_PROFILE table in database.

17.11 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**.

17.12 Mapping the Source Data

Mapping is a way to connect the source data to transaction data and to entities.

17.12.1 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.

17.12.2 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.

17.12.3 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.

17.13 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

17.14 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

17.15 Exporting Transaction Definitions

To export transaction definitions:

1. Navigate to the **Transaction Definitions Search** page, as described in [Section 17.3](#), "[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 17.4](#), "[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.

17.16 Importing Transaction Definition

To import a transaction definition:

1. Navigate to the **Transaction Definitions Search** page, as described in [Section 17.3, "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**.

17.17 Activating a Transaction Definition

To activate a transaction definition:

1. Navigate to the **Transaction Definitions Search** page, as described in [Section 17.3, "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 17.4, "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.

17.18 Deactivating a Transaction Definition

To deactivate a transaction definition:

1. Navigate to the **Transaction Definitions Search** page, as described in [Section 17.3, "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 17.4, "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.

17.19 Deleting Transaction Definitions

To delete transaction definitions:

1. Search for the transaction definition you are interested in, as described in [Section 17.4, "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.

17.20 Use Cases

This section describes example use cases for using transaction definitions.

17.20.1 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 17.1, "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 B.1.4, "Transactions Conditions."](#) Go through the "Possible User Scenarios" section of those rule conditions.
10. For this use case, the rule condition "[Transaction: Check Transaction Aggregate 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 17-2 Transaction Rule Configuration

Parameters	Values
Transaction to check	Choose the transaction definition of Money Transfer
Aggregate Function	Sum
Entity or Element to count	Select the data field that indicates the "money transfer amount"
Condition for Aggregate	Select "Greater Than Equals"
Check value for Aggregate	500
Condition for Count	Greater than Equals
Check Value for Count	1 (since we 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 we 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.

17.20.2 Use Case: Transaction Frequency Checks

These kinds of checks can be implemented using the "[Transaction: Check Transaction Count Using Filter Condition](#)" rule condition. [Table 17-3](#) shows the important parameters of the rule condition.

Table 17-3 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

17.20.3 Use Case: Transaction Frequency and Amount Check against Suspicious Beneficiary Accounts

This kind of check can be implemented using the "[Transaction: Check Transaction Aggregate and Count Using Filter Conditions](#)" rule condition. [Table 17-4](#) shows the important parameters of this rule condition.

Table 17-4 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 Aggregate 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 Aggregate	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

17.20.4 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 17–5 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

17.20.5 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 17–6 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. Let's say we 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 <ul style="list-style-type: none"> ■ 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. Let's say we 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. <ul style="list-style-type: none"> ■ Select Amount data element with condition as "Greater Than" and value as 500

17.20.6 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

Reporting

This part contains information about reporting features in Oracle Adaptive Access Manager 11g.

It contains the following chapters:

- [Chapter 18, "Using the Dashboard"](#)
- [Chapter 19, "Configuring BI Publisher Reports"](#)
- [Chapter 20, "Monitoring Performance by Using Fusion Middleware Control"](#)
- [Chapter 21, "Monitor and Audit of Events"](#)

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](#)

18.1 Introduction

This section introduces you to the dashboard and how it is used.

18.1.1 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.

18.1.2 Common Terms and Definitions

This section contains common dashboard terms and definitions.

- Refresh - the rate to update Dashboard with new data. The choices are 30 seconds, 1 minute, and 10 minutes.
- Performance Panel - 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 - The time frame. The choices are Today, Last 1 day, Last 7 days, Last 30 days, and Last 90 days.
- Average Process Time - Average number of milliseconds for execution.
- Blocked 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

18.2 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.

18.3 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.

18.3.1 Performance

This section provides information on viewing the total view and trending views.

18.3.1.1 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.

18.3.1.2 Viewing Performance Data

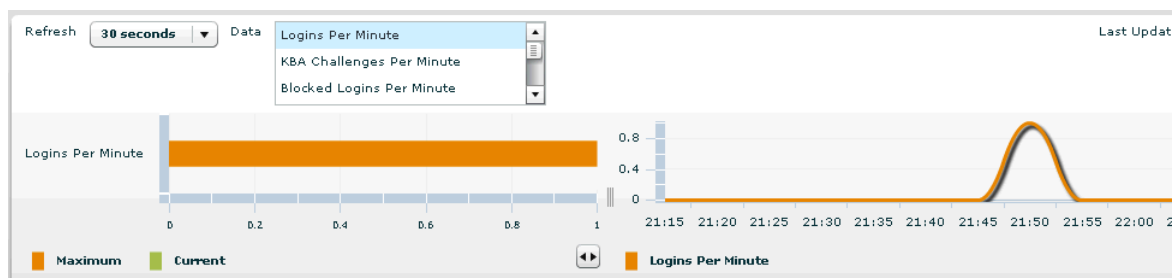
To view the performance data:

1. Select the data type you want from the **Data** list.

The data types provided are:

- 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 18–1 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.

18.3.1.3 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.

18.3.2 Summary

The Summary panel displays an overview or aggregate of the selected data type for the specified range or time frame.

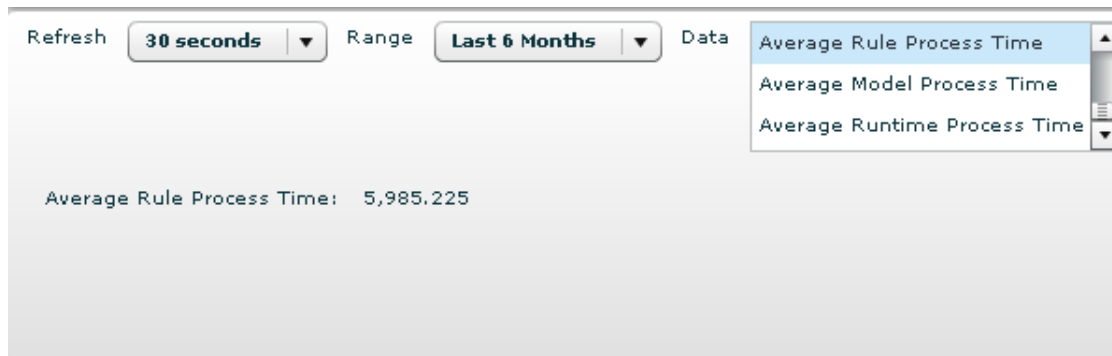
Data Types

The data types provided are:

- Login Sessions - Refers to the login sessions.
- Success Logins - Refers to successful logins.
- Temporary Allow Logins - Refers to logins that occurred while a temporary allow was active.
- Blocked Logins - Refers to logins that were blocked during the login checkpoint.
- High Alert (Logins) - Refers to high level alerts triggered during the login checkpoint.
- KBA Challenges - Refers to challenge question responses.
- OTP Challenges - Refers to OTP challenge responses.
- Transaction Sessions - Refers to Transaction ID.
- Success Transactions - Refers to successful transactions.
- Blocked Transactions - Refers to transactions that were blocked during the transaction checkpoint.
- High Alert (Transactions) - Refers to 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 18–2 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.

18.3.3 Dashboards

Section 3 provides access to five different dashboard types:

- Location

For information about the Location dashboard, refer to [Section 18.3.3.1, "Viewing Data Type by Location."](#)

- Scoring

For information about the Scoring dashboard, refer to [Section 18.3.3.2, "Viewing a List of Scoring Breakdowns."](#)

- Security

For information about the Security dashboard, refer to [Section 18.3.3.3, "Security Dashboard,"](#) and [Section 18.3.3.4, "Viewing a List of Rules or Alerts by Security."](#)

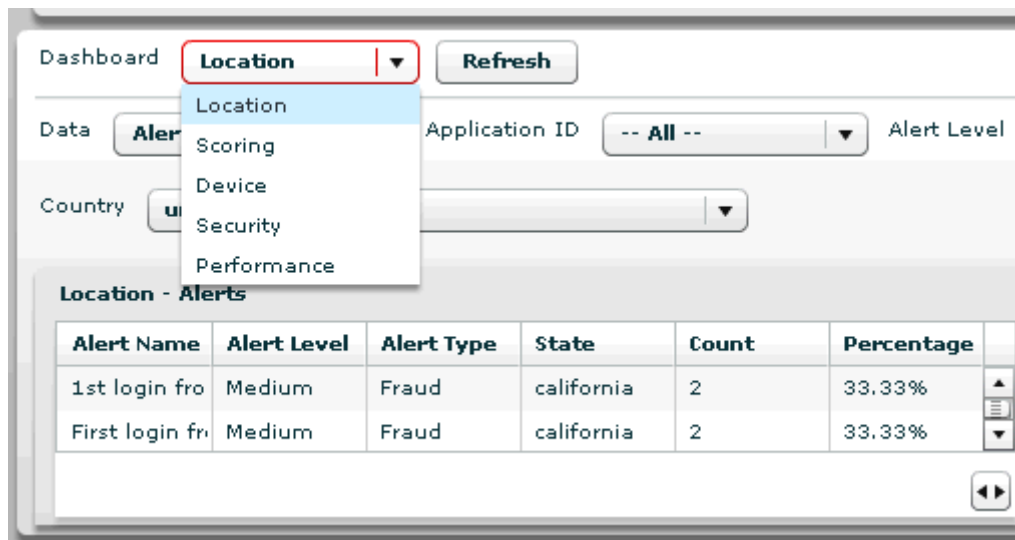
- Device

For information about the Device dashboard, refer to [Section 18.3.3.5, "Viewing Browser and Operating System Data by Device."](#)

- Performance

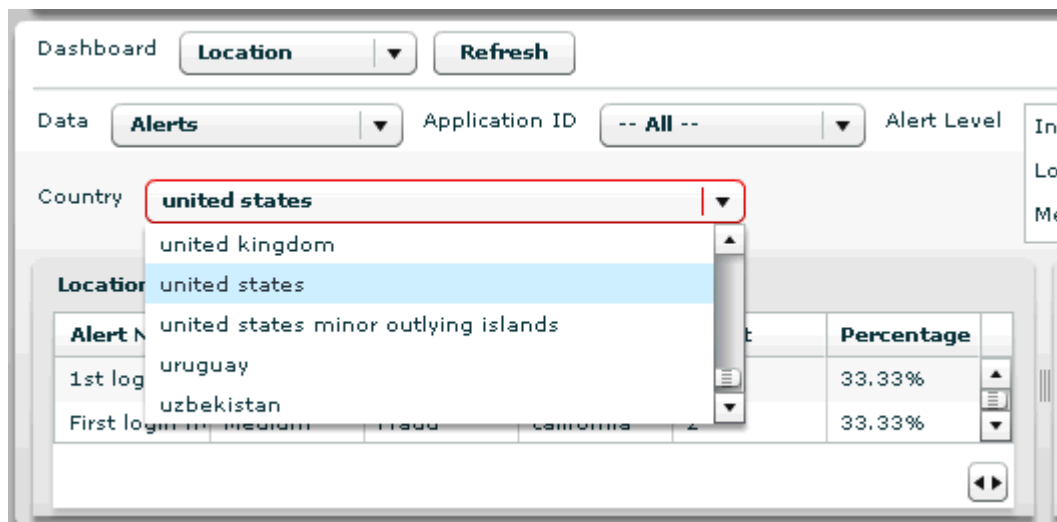
For information about the Performance dashboard, refer to [Section 18.3.3.6, "Viewing a Data Type by Performance."](#)

Figure 18–3 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 18–4 Choices After Data Type Selection



18.3.3.1 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:
 - Alerts - provides a list of alert that have been triggered by country.

- Actions - provides a list of actions that have been taken by country.
 - KBA Challenges - provides a list of KBA challenges that have been triggered by challenge result and country.
 - OTP Challenges - provides a list of OTP challenges that have been triggered by challenge result and country.
 - Routing Type - provides a list of a list of routing types by country.
 - Sessions - provides a list of sessions by country.
 - Temporary Allow - Provides a list of 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.

18.3.3.2 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**.

18.3.3.3 Security Dashboard

Items in the Dashboard list are accessible based on your role. Only fraud investigators can access the Security dashboard.

18.3.3.4 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**.

18.3.3.5 Viewing Browser and Operating System Data by Device

To view browser and operating system data by device:

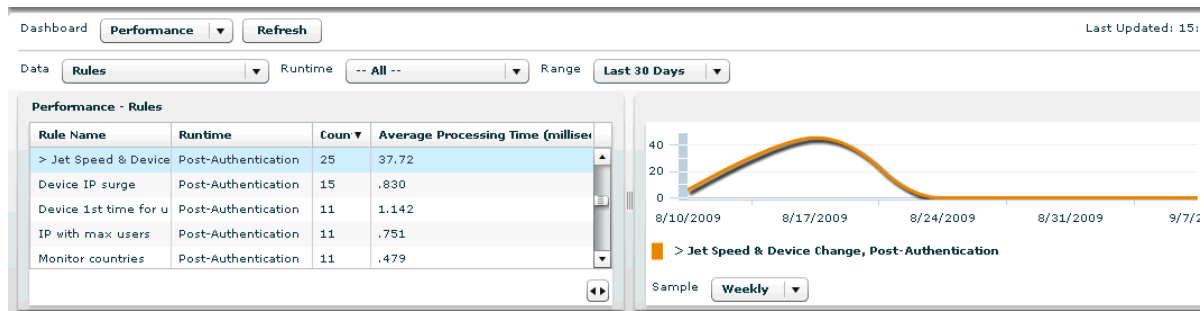
1. In the **Dashboard** list, click **Device**.
The **Device** dashboard appears and defaults to browser/operating system.
2. To narrow the list to a specific **Organization ID**, in the **Organization ID** list, click the Organization ID you want.
3. To narrow the list to a specific timeframe, in the **Ranges** list, click the range you want.
4. Click **Refresh**.

18.3.3.6 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:
 - Rules - The rules currently in the system
 - Policies - The policies currently in the system
 - Checkpoints - The points in a session when rule is run
 - APIs - Calls into the system through the soap interface.
 - Tracker APIs - Calls into the tracker subsystem
 - Authorization APIs - Calls into the authorization subsystem
 - Common APIs - Miscellaneous calls
 - CC APIs - Calls into the Cases subsystem
 - Rules APIs - Calls to the rules processor

Figure 18–5 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**.

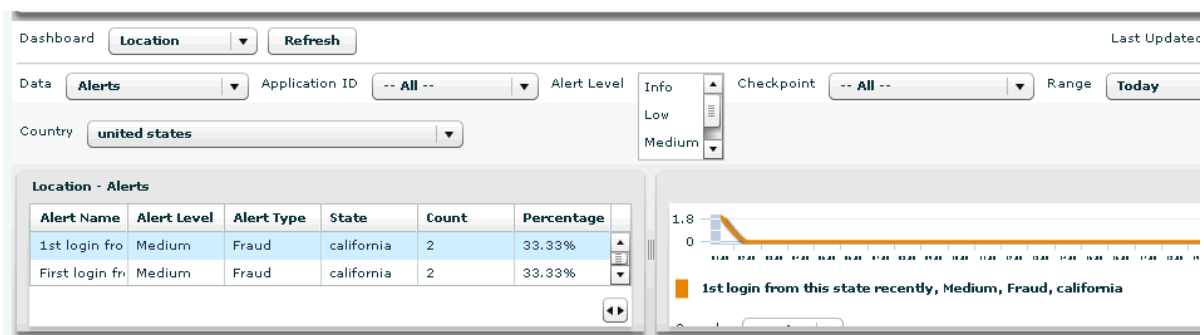
18.3.3.7 Using the Total and Trending Views

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 18–6 Total and trending views



18.3.3.8 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.

18.3.3.9 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.

18.3.3.10 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.

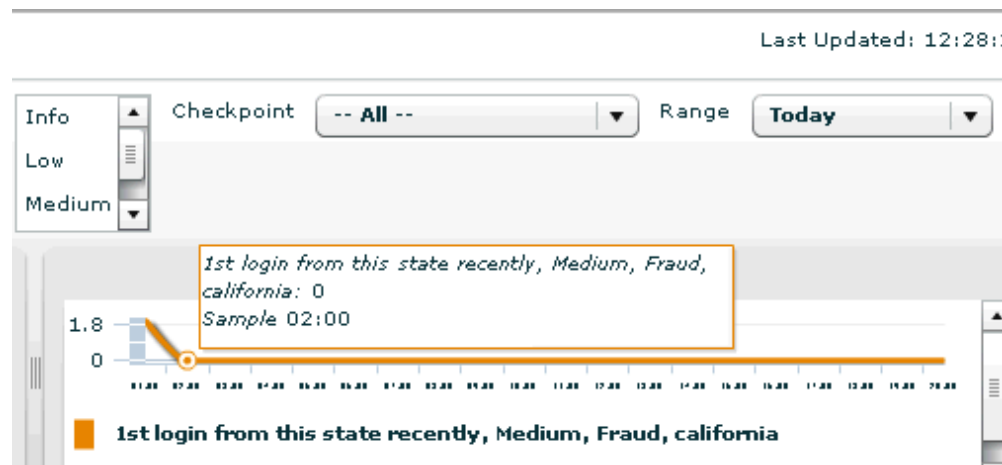
18.3.3.11 Last Updated

The "Last Updated" field, which also appears in the performance panel (Section 1), is updated when you select a different data type.

18.3.3.12 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 18–7 Tooltips



18.4 Use Cases

This section provides a scenario of how Oracle Adaptive Access Manager's dashboards are used.

18.4.1 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.

18.4.2 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.

18.4.3 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.

18.4.4 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

18.4.5 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

Configuring BI Publisher Reports

This chapter describes how to configure reporting and how to view Oracle Adaptive Access Manager reports. It contains these topics:

- [Setting up Oracle Business Intelligence Publisher for Oracle Adaptive Access Manager Reports](#)
- [Viewing/Running Reports](#)
- [Scheduling a Report](#)
- [Example Report Scenarios](#)
- [Best Practices for Creating Reports](#)

19.1 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](#)

19.1.1 Installing BI Publisher

If you do not have Oracle BI Publisher installed, you must install it. Follow the instructions provided at:

http://www.oracle.com/technology/documentation/bi_pub.html

19.1.2 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 the *Oracle Fusion Middleware Business Intelligence Publisher Reports Administrator's Guide for Oracle Identity Management* for more information.

Perform the following steps to install the reports:

1. Download the Oracle Adaptive Access Manager package to your Oracle BI Publisher server. The reports package is available on the Oracle Technology Network web site. You can access the Oracle Technology Network web site at:

<http://www.oracle.com/technology/index.html>

2. Unzip the package to a temporary location on your Oracle BI Publisher server. For example:
 /tmp/OAAM Reports/
3. Stop the Oracle BI Publisher server. Refer to *Oracle Fusion Middleware Business Intelligence Publisher Reports Administrator's Guide for Oracle Identity Management* if you need more information.
4. Recursively copy the /OAAM Reports/Oracle Identity Management Reports/ directory to the /Oracle_BI_Publisher_home/xmlp/XMLP/Reports/ directory on your Oracle BI Publisher server. After performing this step, you should have the following directory on your Oracle BI Publisher server:
 /Oracle_BI_Publisher_home/xmlp/XMLP/Reports/Oracle Identity Management Reports/OAAM/
5. Copy the `properties.xml` file to any directory in Oracle BI Publisher server's file system.
6. Start the Oracle BI Publisher server. Refer to the *Oracle Fusion Middleware Business Intelligence Publisher Reports Administrator's Guide for Oracle Identity Management* if you need more information.

19.1.3 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 Fusion Middleware Business Intelligence Publisher Reports Administrator's Guide for Oracle Identity Management* 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	<code>jdbc:oracle:thin:@host:port:sid</code>
Username	Username for a database schema user that has access to Oracle Adaptive Access Manager.
Password	Password for user identified in the Username field.
Database Driver Class	<code>oracle.jdbc.driver.OracleDriver</code>

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 we placed properties.xml.

The configuration for Oracle Adaptive Access Manager reports is complete. Refer to *Oracle Fusion Middleware Business Intelligence Publisher Reports Administrator's Guide for Oracle Identity Management* to generate reports for Oracle Adaptive Access Manager.

19.1.4 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/xmlpserver/`
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.

19.2 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/xmlpserver/`
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.

19.3 Scheduling a Report

Clicking on the report's **Schedule** button brings up a page which you can use to schedule and administer the report.

You can schedule a report to run on a particular day and time in the future or immediately, once, daily/weekly, or monthly. If you want, you can choose to be notified by email when the report completes or fails.

Perform the following steps to schedule a report:

1. Click the report's **Schedule** button.
2. Set the report parameters:
 - From Date and To Date
 - Format - the output format.
 - Monitor Type
3. Set the job properties:
 - Job Name - a name for your report run.
 - Report Formatting Locale
 - Report Formatting Time Zone
 - Report Formatting Calendar
 - Public - select this checkbox to make this job available to all users with access to the report.
 - Save data for Republish - select this checkbox if you want the XML data from the report run saved.
 - Save Output - select this checkbox if you want the report output saved.
 - Use Unicode (UTF8)
4. In the Notification section, select when you want to be notified and if you want to use email as your notification channel. If you choose email, a field appears for you to provide an email address.
5. Enter the Time criteria.
 - Run Immediately
 - Run Once

- Run Daily/Weekly
 - Run Monthly
6. Select Email in the Delivery section if you want the report sent by email.
 7. Click **Submit**.

19.4 Example Report Scenarios

The following are some example reporting scenarios. The exact reporting practices used by each institution may differ based on company policies. If a separate reporting database is not being used, great care must be taken when running reports on a live production system. All but the narrowest queries should be scheduled to run during off hours in this case.

One useful strategy is to schedule a general alert based report for each application on a nightly basis. Any suspicious activity should be further investigated using narrow queries and detail screens. Specific queries used for targeted investigation can be found in the query types menus under each of the three query families (User, Location, Device).

19.4.1 Example General Nightly Report

User/Recent logins - Schedule this report to run with the following parameters

Check Alert Level - ALERT_MEDIUM and ALERT_HIGH

Organization ID- The user group associated to the application

Scheduled Report

- Frequency - Day
- Range - Last 24 hours

Example Scenario 1

Nightly the User/Recent logins report is scheduled to run for the last 24 hours. One day the report shows several "Multiple failures from the device" alerts. The investigator could run a narrow query then view detail screens to gain more information. To see if the behavior that triggered the rule has been happening with a wider threshold further targeted reports could be scheduled for the next night.

19.4.1.1 User/Recent Logins

Run this narrow query with one of the specific session IDs in which the "Multiple failures from the device" alert was triggered. This session ID is the first number shown in each session listing in the general nightly report that was scheduled.

19.4.1.2 Device details

After running the narrow recent logins query the details screens associated with the login session can be viewed. These detail screens have a wealth of information collected by Oracle Adaptive Access Manager that can be used in an investigation. For example, customers attempting logins from the suspect device can be seen on the device details screen under the users tab. If desired, action outside of Fraud Analyzer can be taken to investigate these customers for more information. For example, customers could be called to see if they have been experiencing problems accessing their account. Action from here should be guided by your institution's policies.

19.4.1.3 Device/Multiple Failures

A targeted report could be scheduled to run in response to the activity seen in the general report if a deeper look into the data is desired. Schedule this targeted report with the threshold values a bit higher than the specific rule that was triggered the previous day. The session details screen for each session ID will show what rules were triggered and there are links to the model edit screen where the exact thresholds of the rules can be seen. Any devices with exceptionally high numbers of failures should be looked into using their device details screens. Some example values are listed as follows:

Min No. Of Login Failures - 15

From and To Dates - a range corresponding to the last 48 hours

Scheduled Report

- 2 am

Example Scenario 2

Nightly the User/Recent logins report is scheduled to run for the last 24 hours. One day the report shows a "Login from restricted country" alert. The investigator could run a narrow query then view detail screens to gain more information. To see if the behavior that triggered the rule has been happening with a wider threshold further targeted reports could be scheduled for the next night.

19.4.1.4 User/Recent Logins

Run this narrow query with the specific session ID in which the "Login from restricted country" alert was triggered. This session ID is the first number shown in each session listing in the general nightly report that was scheduled.

19.4.1.5 Location details

After running the narrow recent logins query the details screens associated with the login session can be viewed. These detail screens have a wealth of information collected by Oracle Adaptive Access Manager that can be used in an investigation. For example, customers attempting logins from the suspect countries can be seen on the location details screen under the users tab. If desired, action outside of Fraud Analyzer can be taken to investigate these customers for more information. For example, customers could be called to see if they have been accessing their accounts from outside of the USA. Action from here should be guided by your institution's policies.

19.4.1.6 Location/Users by Location

A targeted report could be scheduled to run in response to the activity seen in the general report if a deeper look into a single location is desired. Schedule this targeted report with a specific IP or geographic location. Any users found to be attempting logins from restricted countries should be looked into. Here are some example values that could be used.

Country Name X

From and To Dates - a range corresponding to the last 48 hours

Scheduled Report

- 2 am

19.4.2 Additional Sample Analyses

Similar to the analysis processes earlier, other reports can be used to investigate specific situations. Here are some more examples of useful reports to run after viewing the following alerts.

- If the "Multiple Logins from IP" alert is triggered, run **Location - Multiple Users** report to see if there were any IPs recently that had a high number of users.
- If the "Multiple users are using the same device in short time frame" alert is triggered, run **Device - Multiple Users** report to see if there were any devices recently that had a high number of users with specific IP or geographic location parameters.
- If the "Login from restricted device" alert is triggered, run the **Device - Users by Device** report which will show the users that used a restricted device to log in.

19.4.2.1 Here are some example values that could be used.

Specific IP or a Geographic location

From and To Dates - a range corresponding to the last 48 hours

Scheduled Report

- 2 am

19.4.2.2 Device/ Users by Device

If the "Login from restricted device" alert is seen in a nightly report this targeted report could be run the next night. This report will show the users that used a restricted device to login. Here are some example values that could be used.

Device Group - Restricted Devices

Group ID - Default user group for the application

From and To Dates - a range corresponding to the last 48 hours

Scheduled Report

- 2 am

19.5 Best Practices for Creating Reports

Customer Statistic	Reports	Directions	Notes
identify Kiosk/public computers	Device/Multiple Users	Turn up minimum number of users to an exceptional level to detect devices with extremely high numbers of users.	
How many incorrect usernames are entered per month?	User/Invalid Logins	Set min number of attempts to 1 and the time range to a month	

Customer Statistic	Reports	Directions	Notes
Identify users that use a very high number of computers to log in	User/Multiple Devices	Turn up minimum number of devices to an exceptional level to detect users with high numbers of devices.	The customer profile rules could be adjusted if it is discovered that the majority of users use more than the maximum allowed devices
Identify new online users	User/First Login User/Frequent Logins		
Identify the number of users having problems logging in	User/Multiple Failures	Set min number of attempts to a low number like 3 and the time range to one month	This will give a general idea of the difficulty users are having successfully logging in. However, hacker activity can skew these numbers

Hacker Issues	Reports	Notes
Brute Force		
locate possible brute force attacks	Device/Multiple Failures	Turn up minimum number of failures to an exceptional level to detect devices failing to log in an abusive number of times.
	User/Multiple Failures	Turn up minimum number of failures to an exceptional level to detect users failing to log in an abusive number of times.
	Location/Multiple Failures	Select a location and increase minimum number of failures to an exceptional amount.
	User/Multiple Devices	Turn up minimum number of devices to an exceptional level.
	Location/Invalid Users	Turn up minimum number of attempts to an exceptional level.

19.6 Use Cases

The following section provides a scenario of how Oracle Adaptive Access Manager's reports are used.

19.6.1 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.

19.6.1.1 Description

This use case demonstrates how to use BI Publisher.

19.6.1.2 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**.

Monitoring Performance by Using Fusion Middleware Control

This chapter describes how to monitor Oracle Adaptive Access Manager 11g performance and shut down and start Oracle Adaptive Access Manager instances using Fusion Middleware Control.

20.1 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:

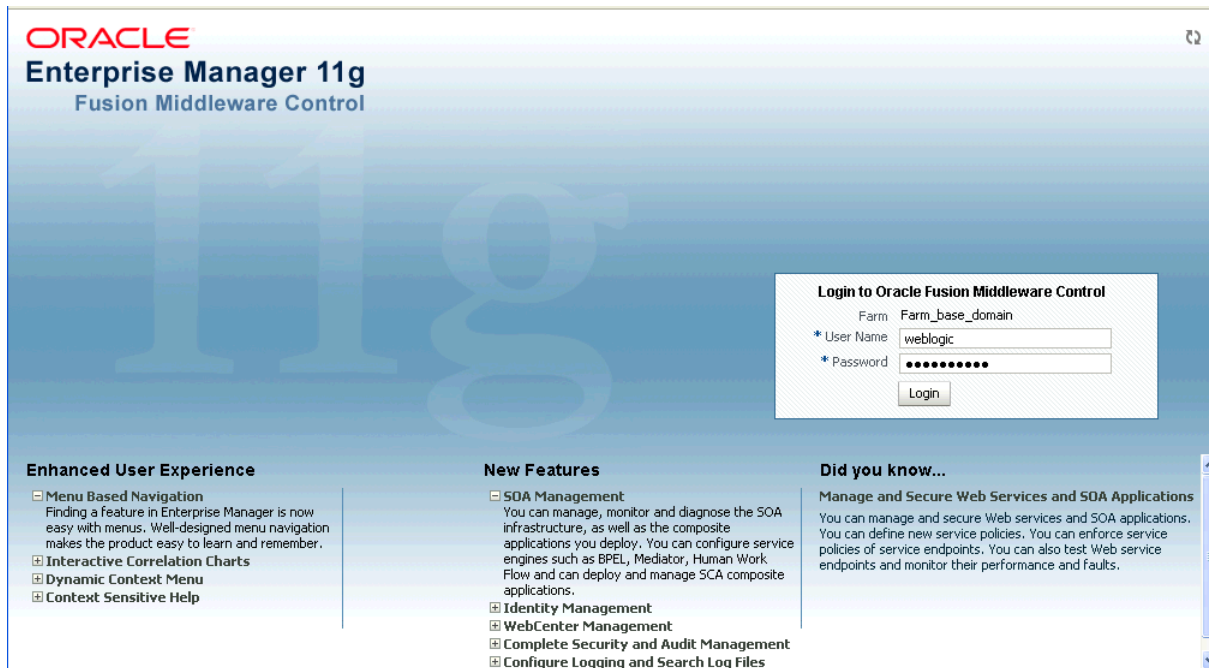
```
http://hostname.domain:port/em
```

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 20-1](#).

Figure 20–1 Fusion Middleware Control Login



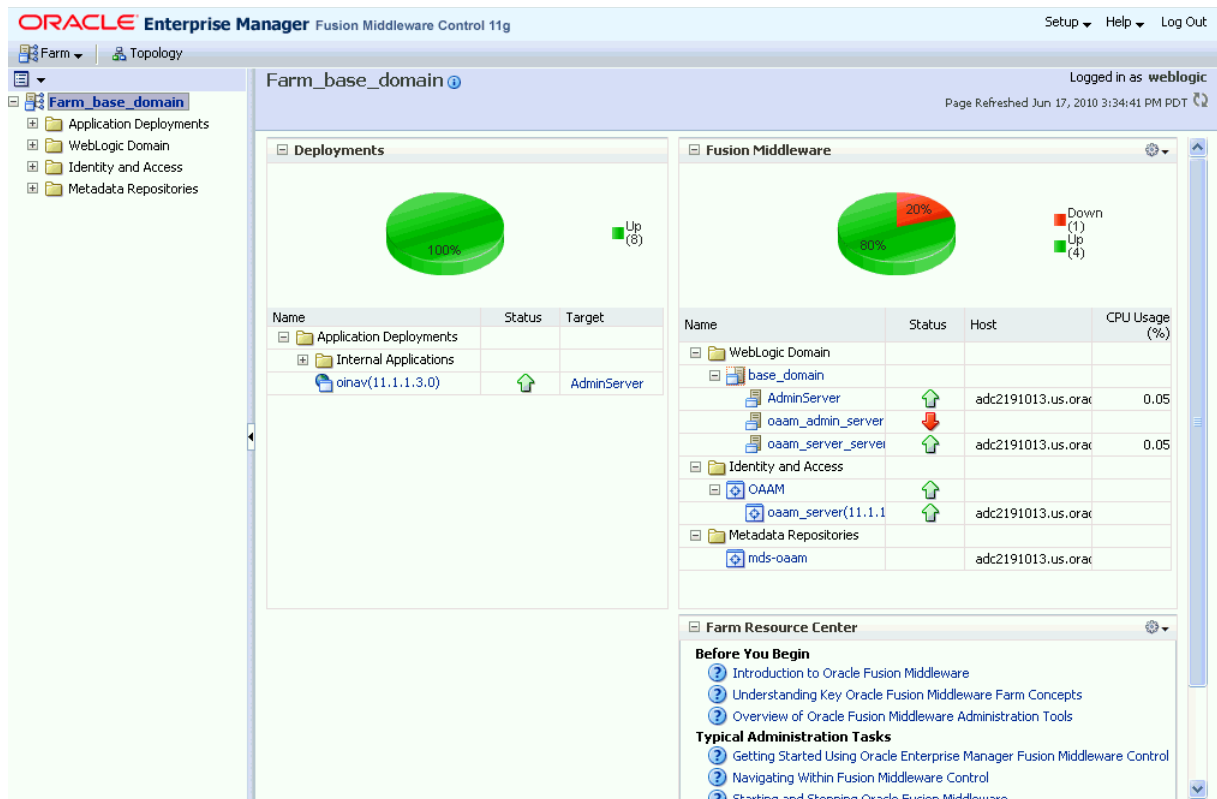
20.2 Displaying Base Domain 11g Farm Page

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 20–2](#)

Figure 20–2 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:

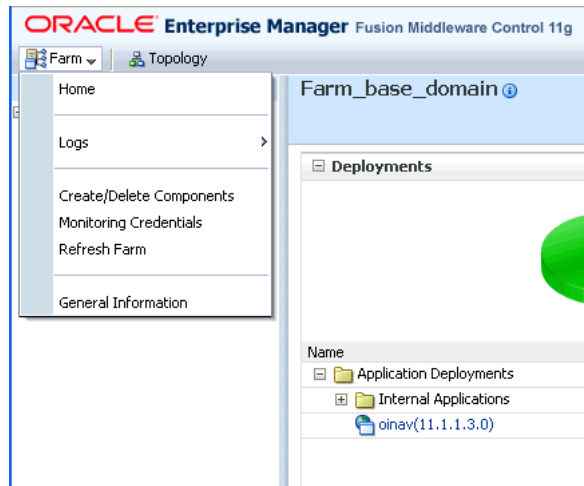
- Application Deployments
- WebLogic Domain
- Identity and Access
- Metadata Repositories

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.

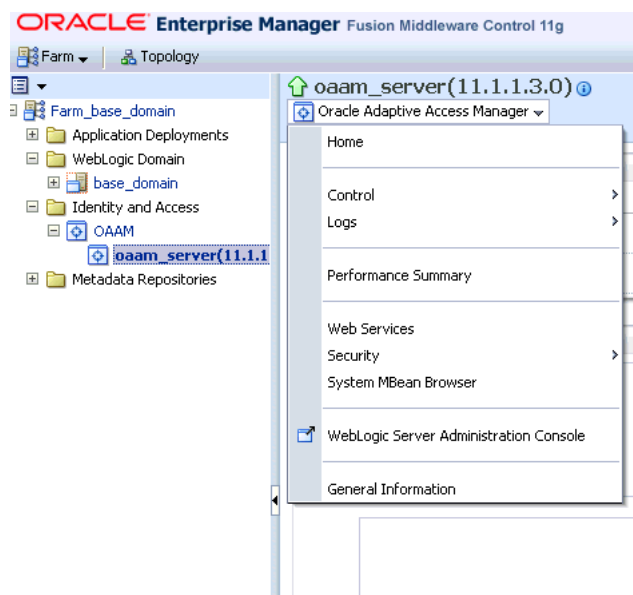
Figure 20–3 Farm Menu



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 20–4 Dynamic Menu



20.3 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: <ul style="list-style-type: none"> ■ Green Up Arrow indicates that the instance is running ■ Red Down Arrow indicates that the instance is not running ■ 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**.

20.4 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	<p>Allows you to view a performance summary</p> <p>From the menu, click Performance Summary.</p> <p>The categories for the summary metrics are:</p> <ul style="list-style-type: none"> ■ CheckPoint Execution Summary ■ Login Metrics Summary ■ Policy Execution Summary ■ Rule Execution Summary ■ Rule Processing Summary ■ Update Authorization Status Summary ■ Update Log Summary ■ Web Module Metrics
Web Services	<p>Allows you to view web services</p> <p>From the menu, click Web Services.</p>
Security	<p>Allows you to view OAAM Server application policies and roles</p> <p>From the menu, click Security and select Application Policies or Application Roles.</p>
System MBean Browser	<p>Allows you to access the System MBean Browser</p> <p>From the menu, click System MBean Browser.</p>
WebLogic Server Administration Console	<p>Allows you to access the WebLogic Server Administration Console</p> <p>From the menu, click WebLogic Server Administration Console.</p>
General Information	<p>Allows you to view general information about the server instance</p> <p>From the menu, click General Information.</p>

Monitor and Audit of Events

This chapter contains the following sections:

- [Monitoring Information Sent to Dynamic Monitoring System](#)
- [Audit Information Sent to Audit System](#)

21.1 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):

21.1.1 Login Information (Counts Only)

Login Information (Counts only) that is sent are:

Table 21–1 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

21.1.2 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 21–2](#).

Table 21–2 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

21.1.3 APIs Execution Information (Count and Time Taken to Execute)

The APIs execution information (count and time taken to execute) is shown in [Table 21–3](#)

Table 21–3 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

21.2 Audit Information Sent to Audit System

Oracle Fusion Middleware Audit Framework is a new service in 11g 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 11g logs the following events using the Oracle Audit Framework:

21.2.1 Customer Care Events

Customer Care Events are shown in [Table 21–4](#).

Table 21–4 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	

21.2.2 Policy Management Events

Policy Management Events are listed in [Table 21–5](#).

Table 21–5 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	

21.2.3 KBA Questions Events

KBA Questions Events are listed in [Table 21–6](#).

Table 21–6 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	
Update KBA Validation	KBAValidationId, KBAValidationName, KBAValidationDetails	
Delete KBA Validation	KBAValidationIds	
Add KBA Validation to Global	KBAValidationId	

Table 21–6 (Cont.) KBA Questions Events

Event Name	Event Data	Notes
Delete KBA Validation from Global	KBAValidationId	
Update KBA Answer Logic	KBAAnswerLogicDetails	
Update KBA Registration Logic	KBARegistrationLogicDetails	

21.2.4 Group/List Management Events

Group/List Management Events are listed in [Table 21–7](#).

Table 21–7 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 VIII

Deployment Management

This part of the book contains information about managing deployment in Oracle Adaptive Access Manager.

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](#)

22.1 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.

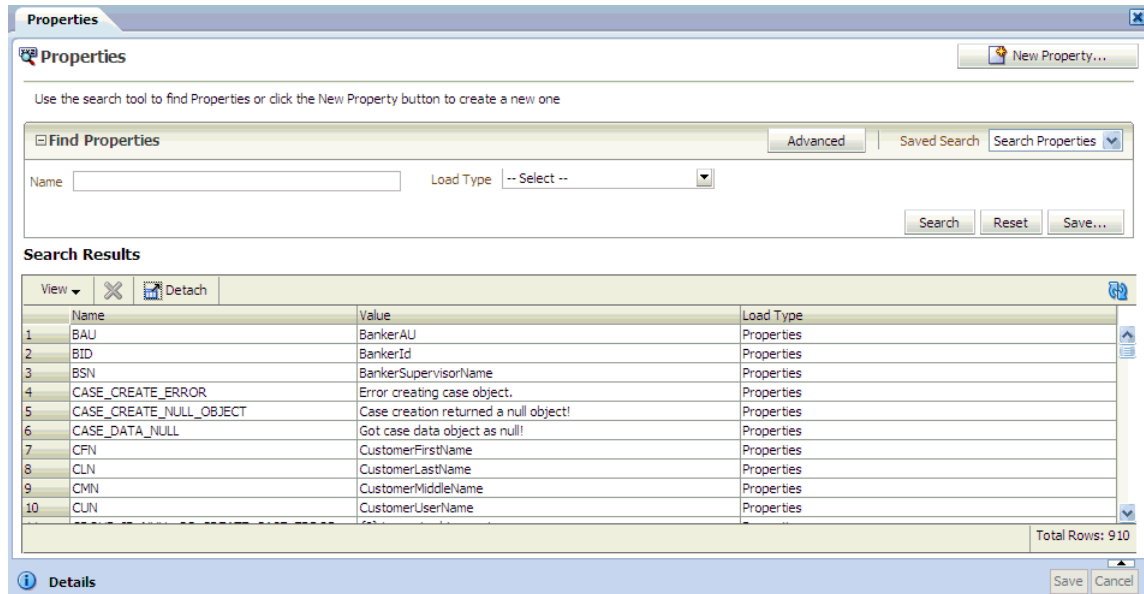
The Properties Search page is displayed.

2. Click **Search** to view a list of properties in the system.

22.2 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 22–1 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 22–1, " Search Filter Criteria"](#).

Table 22–1 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.

22.3 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.

22.4 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
```

22.5 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 255 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**.

22.6 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.

22.7 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.

22.8 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.

22.9 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 IX

Command-Line Interface

This part describes how to set up and use Oracle Adaptive Access Manager's command-line interface.

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](#)

23.1 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

23.2 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

23.2.1 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.

23.2.2 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

23.2.2.1 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
<code>oaam.csf.useMBeans</code>	false
<code>oaam.jps.config.filepath</code>	Set the absolute path of <code>jps-config-jse.xml</code> . Usually, it resides in <code>\$DOMAIN_HOME/config/fmwconfig</code> folder

2. Open the file, `conf/bharosa_properties/oaam_core.properties` in a text editor and set the following properties related to the Oracle Adaptive Access Manager database:

Property Name	Notes about Property Values
<code>oaam.db.url</code>	Specify valid JDBC URL of the Oracle Adaptive Access Manager database. Make sure there are no typos.
<code>oaam.db.additional.properties.file</code>	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 <code>oaam_core.properties</code>

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)

3. Make sure the following jar files are set in Java classpath environment variable.

Path	Required Jars
\$WL_HOME\oracle_common\modules\oracle.jps_11.1.1	<ul style="list-style-type: none"> ▪ jps-api.jar ▪ jps-common.jar ▪ jps-internal.jar
\$WL_HOME oracle_common/webservices/wsclient_extended.jar	wsclient_extended.jar
\$WL_HOME/oracle_common/modules/oracle.iau_11.1.1	fmw_audit.jar

23.2.2.2 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 CSR 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	<Username 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_core.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_core.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)
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)

3. Make sure the following jar files are set in Java classpath environment variable.

Path	Required Jars
\$WL_HOME\oracle_common\modules\oracle.jps_11.1.1	<ul style="list-style-type: none"> ▪ jps-api.jar ▪ jps-common.jar ▪ jps-internal.jar
\$WL_HOME\wlserver_10.3\server\lib	<ul style="list-style-type: none"> ▪ wlclient.jar ▪ wljmxclient.jar
\$WL_HOME/oracle_common/modules/oracle.iau_11.1.1	fmw_audit.jar

23.2.3 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 >"/>
```

23.3 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 23.2, "Setting Up the CLI Environment."](#)

23.3.1 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 runImportExport.sh script without any arguments.

```
$ sh runImportExport.sh
```

23.3.2 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.

23.3.2.1 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 >

```

23.3.2.2 CLI Parameters

The options are described in [Section 23.3, "Using CLI."](#)

Table 23–1 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 or 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.

23.3.2.3 Supported Modules for Import and Export

The list of supported modules for Oracle Adaptive Access Manager 11g is shown in [Table 23–2](#).

Table 23–2 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 10g policy set and policy modules are not longer valid in 11g.

The difference between CLI import/export in 10g and 11g is that the module `models` and `policies` means the same: `-module policy` is same as `-module models`.

23.3.2.4 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`).

23.3.2.5 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.

23.3.2.6 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
```

23.3.2.7 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 modell.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.

23.3.2.8 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
```

23.3.2.9 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.

23.3.2.10 Upload Location Database

To use the IP location loader utility, follow the setup instructions in [Section 23.4, "Importing IP Location Data."](#)

23.3.3 Globalization

For this release, CLI is not globalized.

23.4 Importing IP Location Data

This section describes a utility for importing the 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 File Layout](#)
- [Oracle Adaptive Access Manager Tables](#)
- [Verifying When the Loading was a Success](#)

23.4.1 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 23.2, "Setting Up the CLI Environment."](#)

23.4.1.1 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=6d483869-816a-44cb-9787-a866235efc7c&DisplayLang=en>

23.4.1.2 Setting Up IP Location Loader Properties

1. 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 in the following properties. The location data should be obtained from one of the supported vendors (`ip2location`, `maxmind`, `quova`).

Note that the properties marked as "Advanced" are not to be changed in general.

Table 23-3 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
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

23.4.1.3 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
```

23.4.1.4 Setting Up Encryption

Refer to [Chapter 2, "Setting Up the Oracle Adaptive Access Manager Environment"](#) for information on setting up encryption.

23.4.1.5 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.

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.

23.4.2 System Behavior

The IP location loader utility reads the information from the IP location data files (from Quova 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 `vdecrypt_ip_location_map` for each record in the data file. It also creates a new record in `vdecrypt_country` for each unique country name in the data file, a new record in `vdecrypt_state` for each unique combination of country name and state name in the data file, and a new record in `vdecrypt_city` for each unique combination of country name, state name, and city name in the data file.

When the IP location loader utility 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 `vdecrypt_ip_location_map` table. It creates a new row in the `vdecrypt_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 `vdecrypt_ip_location_map` whose `FROM_IP_ADDR` matches the record in the data file, but has different data in other columns. The utility also creates new countries, states, and cities that do not already exist in the database.

23.4.3 Quova File Layout

The Quova 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's GeoPoint Data Glossary. In the following table, IP represents the `vdecrypt_ip_location_map` table, CO represents the `vdecrypt_country` table, ST represents the `vdecrypt_state` table, and CI represents the `vdecrypt_city` table.

The file layout is as follows:

Table 23–4 Quova File Layout

Quova 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 <code>vdecrypt_ip_location_map</code> 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 longitude of the IP address. Positive numbers represent East, and negative numbers represent West.

Table 23–4 (Cont.) Quova File Layout

Quova Field	Oracle Adaptive Access Manager Field	Description
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)	
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 reference file.
Top Level Domain	mapped to IP.top_level_domain	The top level domain of the URL. For example,. com in www.oracle.com. This is mapped through the Quova reference file.
Registering Organization	(not used)	

23.4.3.1 Routing Types Mapping

A table for routing types mapping is shown in [Table 23–5](#).

Table 23–5 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.

Table 23–5 (Cont.) Routing Types Mappings

Routing Type	Oracle Adaptive Access Manager ID	Description
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.
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.

23.4.3.2 Connection Types Mapping

Table 23–6 shows connection types mappings.

Table 23–6 Connection Types Mappings

Connection Type	Oracle Adaptive Access Manager ID	Description
ocx	1	This represents OC-3 circuits, OC-48 circuits, etc. 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.

Table 23–6 (Cont.) Connection Types Mappings

Connection Type	Oracle Adaptive Access Manager ID	Description
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, etc. In general ranges in speed from 256k to 20MB per second.
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.

23.4.3.3 Connection Speed Mapping

Table 23–7 shows connection speed mappings.

Table 23–7 Connection Speed Mappings

Connection Speed	Oracle Adaptive Access Manager ID	Description
high	1	OCX, TX, and Framereley.
medium	2	Satellite, DSL, Cable, Fixed Wireless, and ISDN.
low	3	Dialup and Mobile Wireless.
unknown	99	Quova was unable to obtain any line speed information.

23.4.4 Oracle Adaptive Access Manager Tables

This section contains the tables used by the ETL process

23.4.4.1 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 23–8 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

23.4.4.2 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

23.4.5 Verifying When the Loading was a Success

The loader script returns 0 when the data load is successful; on failure it returns 1.

Part X

Multitenancy

This part of the book provides concepts on multitenancy in Oracle Adaptive Access Manager

It contains the following chapter:

- [Chapter 24, "Multitenancy"](#)

Multitenancy

Multitenancy refers to a principle in software architecture where a single instance of the software runs on a server, serving multiple client organizations (tenants).

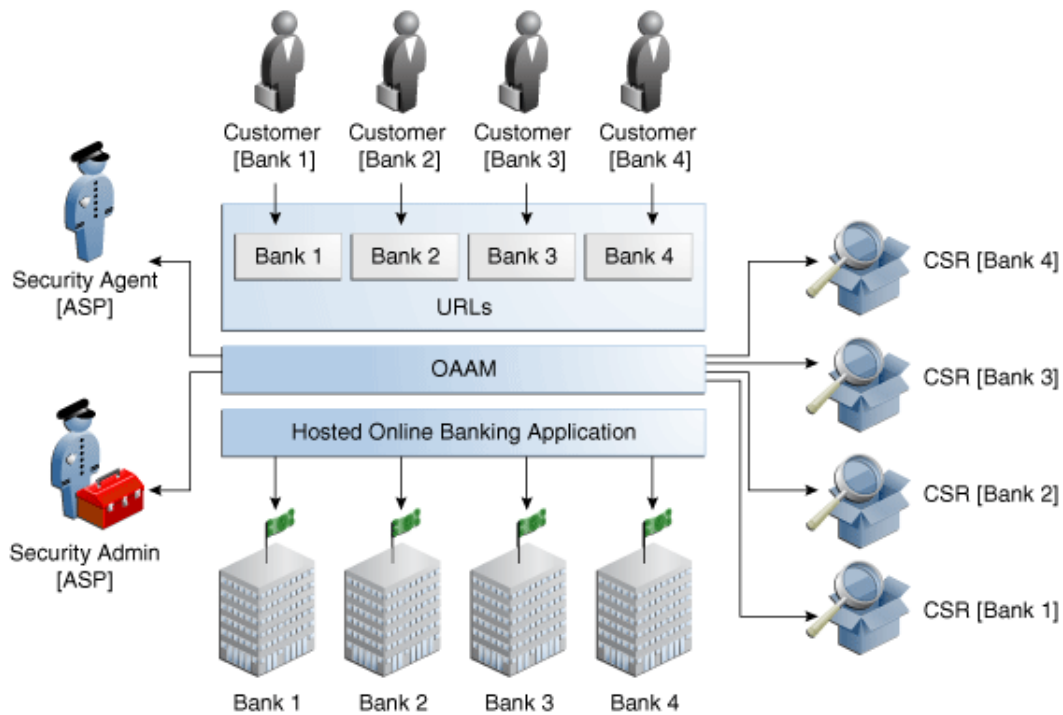
With a multitenant architecture, a software application is designed to virtually partition its data and configuration so that each client organization works with a customized virtual application instance.

The distinction between the customers is achieved during application design, so that customers do not share or see each other's data.

Oracle Adaptive Access Manager by default is enabled for multitenancy. A single shared instance of Oracle Adaptive Access Manager can support multiple tenants. Policies and rules can be centrally administrated and can be shared between applications, with the option to personalize for individual applications.

24.1 Multitenancy Scenario

[Figure 24-1](#) shows a multitenancy scenario.

Figure 24–1 Multitenant SaaS**Shared Infrastructure/Shared Application**

In the example shown in [Figure 24–1](#), the online banking application (same instance of the same server) is divided into virtual instances used by different tenants.

Awareness of the Applications

Each "application" corresponds to an Application ID: Bank1, Bank2, Bank3, and Bank4.

The online banking application can be customized by organizations as though each organization had a separate application.

The shared application presents the appropriate interface to any particular tenant at any given time. If the customer tries to access Bank1, a personalized customized interface for Bank 1 appears.

Access Control for All of Users Involved

Customers who use the "applications" are Customer (Bank 1), Customer (Bank2), Customer (Bank 3), and Customer (Bank 4).

The data and customizations are insulated from all of the other tenants.

24.2 Changes in Terminology

Some key terminology used in the 10g has changed in 11g. [Table 24–1](#) shows the changes.

Table 24–1 Terminology Changes

For Deployed Application	10g terminology	11g terminology
OAAM Admin Console	Primary user group	Organization ID
OAAM Admin Console	Application ID	Organization ID
OAAM Server	Application ID	Remains same as 10g

Organization ID

Each end-user belongs to a single Organization ID. Multiple applications can be mapped to an Organization ID. The opposite is not true however.

Application ID

The Application ID is a transient value that uniquely identifies an application to allow specific control of the user experience. Application ID remains unchanged in 11gR1.

Deprovisioning

Users can not be easily removed from an Organization ID. Deprovisioning can be accomplished handled through native integration APIs only.

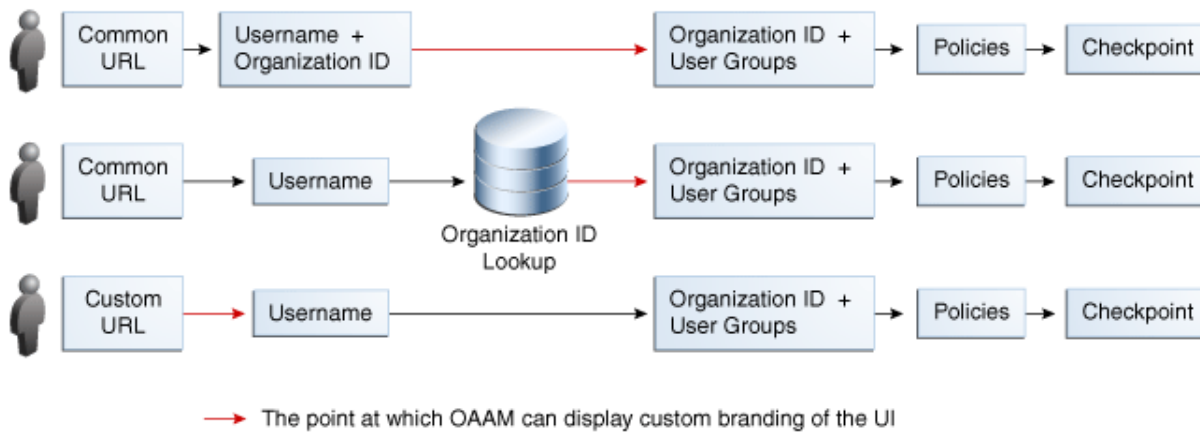
24.3 Mapping of Application ID (Client-Side) to Organization ID (Administration Side)

To ensure that customer 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.

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.

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, user enters his user ID, which is mapped to an Organization ID.

Figure 24–2 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 (which pages the organization and policy map to).

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.

24.4 Multitenant Support In Oracle Adaptive Access Manager

For areas other than case management, data access filtered on organization ID is not supported currently. Oracle Adaptive Access Manager cannot control the data administration and security personnel view in the Admin Console.

Policy scoping can be accomplished for specific subgroups of tenants to who use the same applications; user groups can be configured to categorize these populations of users.

These user groups must be manually maintained. Autoprovisioning is not available for the groups.

Part XI

Troubleshooting

This part provides information for troubleshooting symptoms and gives solutions to the difficulties you may experience.

This chapter describes common troubleshooting issues and tips to resolve them.

25.1 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 show 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 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 recognizes the files successfully.

There is no issue if the MIME entry is already present in operating system.

25.2 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 we 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).

25.3 Globalization

Character set 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.

25.4 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:

```
customer_care.case.actiontype.enum.accesscase.description=Access case
```

Case creation / access logic will use that string for the creating records after that point.

Common problems and activities in customer services

Question/Problem: What are common problems and activities in customer services?

Answer/Solution: Common problems and actions are listed in this table.

Problem	Possible Reason	Action to Perform
Customer cannot log in	Customer forgot challenge question answers	Reset challenge questions Refer to Section 4.11.2, "Resetting Challenge Questions."
	Customer did not register	Inform customer that registration is required at the next login.
	Customer traveling and attempting to log in from a blacklisted country and the system has blocked him.	Grant temporary allow Refer to Section 4.12, "Enabling a Temporary Allow (CSR Manager Only)."
Customer locked out of the system	"Locked" is the status that Oracle Adaptive Access Manager sets if the user fails a challenge. The "Locked" status is only used if the KBA or One Time Password (OTP) facility is in use. <ul style="list-style-type: none"> ■ OTP: Customer exceeds the number of retries when attempting to put in his OTP code, his account becomes "Locked." ■ KBA: For online challenges, customer reaches the maximum number of failures for his online counter. For phone challenges, customer reaches the maximum number of failures and no challenge questions are left. 	Reset the status to "Unlocked" before the account can be used to enter the system Refer to Section 4.10.7, "Unlock OTP." Refer to Section 4.11.5, "Unlocking a Customer (KBA)."
	Customer blocked from performing transactions	A customer might be in a restricted users group that is intended for users who have had high risk activity. If the user has not performed any high risk activity recently, the security team might want to remove this user from the restricted users group.
Customer calls with a new problem		Open case Refer to Section 4.8, "Creating a CSR Case."
Customer does not like the virtual device personalization registered		Reset the image and phrase. Refer to Section 4.10.3, "Resetting Image and Phrase."
Customer does not like the virtual authentication device he has registered		Reset virtual authentication device. Refer to Section 4.10.6, "Resetting Virtual Authentication Device."
Customer forgot the answers to the registered questions		Reset questions Refer to Section 4.11.2, "Resetting Challenge Questions."
Customer does not want his device to be flagged as "safe."	Customer no longer uses the device	Unregister device Refer to Section 4.10.4, "Unregistering Devices."

25.5 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 6.9.3, "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.

25.6 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.

25.7 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.

25.8 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 UI, 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.

25.9 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 Username group

Question/Problem: What is the difference between a user ID and a Username group?

Answer/Solution: The Username 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.

25.10 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.

25.11 Autolearning

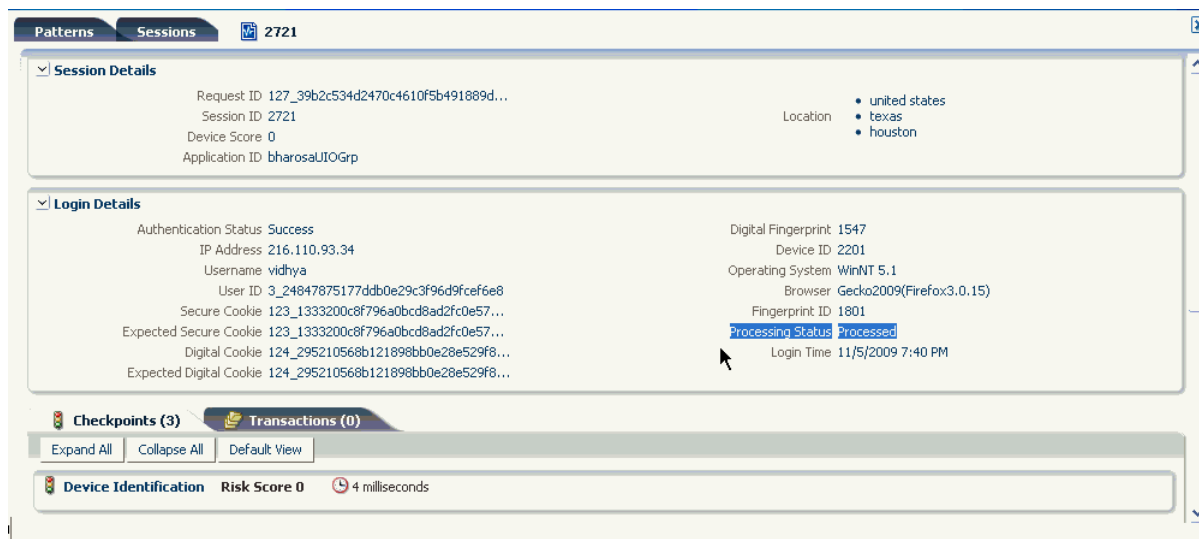
Verify that autolearning is functional

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 25–1 Autolearning processing



If autolearning has not been set up correctly, data will not have been processed.

25.12 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 16.9, "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 16.6, "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 16.11, "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

25.13 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.

25.14 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.

25.15 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's 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 23, "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.
For information on creating a cron job, refer to <http://en.wikipedia.org/wiki/Cron>
3. Ensure that you:
 - a. Encrypt the database password. Refer to [Chapter 23, "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.

25.16 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;
```

25.17 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 we need to decrypt the data? When do we 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 we omit the encryption?

Answer/Solution: SOAP is optional. Database and System are mandatory

25.18 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 18, "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 C, "Oracle Adaptive Access Manager Reports Reference."](#)

25.19 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.

Part XII

Appendixes

This section contains the following reference appendixes:

- [Appendix A, "Pattern Processing"](#)
- [Appendix B, "Conditions Reference"](#)
- [Appendix C, "Oracle Adaptive Access Manager Reports Reference"](#)
- [Appendix D, "Oracle Adaptive Access Manager Properties"](#)
- [Appendix E, "The Discovery Process"](#)
- [Appendix F, "Globalization Support"](#)
- [Appendix G, "Setting Up Archive and Purge Procedures"](#)
- [Appendix H, "Configuring Logging Output"](#)
- [Appendix I, "Rule and Fingerprint Logging"](#)
- ["Glossary"](#)

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.

A.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 we 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.

A.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.

A.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 A-1 *updateTransaction Parameter and Returned Value*

Parameter	Description
TransactionUpdateRequestData	<p>The object to update a transaction; a handle to the transaction to be updated is either the transaction ID returned by the method <code>createTransaction</code>, or the external transaction ID passed to the method <code>createTrasnaction</code>. it throws the exception <code>BharosaException</code> if it fails validation.</p> <p>The structure of this object is as follows:</p> <ul style="list-style-type: none"> ▪ <code>requestId</code>, identifies the user session; required ▪ <code>requestTime</code>, the time of the request; can be null; if null, the server uses the current time ▪ <code>transactionId</code> ID, the ID returned by a previous call to <code>createTransaction</code> ▪ <code>status</code>, the transaction status ▪ <code>analyzePatterns</code>, 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." ▪ <code>externalTransactionId</code>, the external transaction ID that was passed to <code>createTransaction</code> when the transaction was created
VCryptResponse	<p>The response object; make sure to check <code>isSuccess()</code> before obtaining the transaction ID with the method <code>getTransactionResponse()</code></p>

A.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 A-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."

A.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 A-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.

Conditions Reference

This appendix provides information about the conditions available standard on Oracle Adaptive Access Manager.

Condition Name	Condition Description
Always On - User	This rule is always processed
Device: Browser header substring	Checks to see if the supplied string exists as a substring in the browser's header information
Device: Device in list	Checks to see if the device is in the list
Device: Device first-time for user	Checks to see if the device is used for the first time by the user
Device: Excessive use	Device is excessively used that has not been used before
Device: Is registered	Checks to see if the user has registered the device
Device: Login Count	Checks to see if unique user count using this device in past "x" seconds
Device: Timed not status	Maximum login attempts for all but the given status within the given time period
Device: Used count for user	Device used count. This condition ignores the current request for calculating the device count.
Device: User status count	Checks user count with the given status from this device in the specified duration
Device: Velocity from last login	Triggers when miles per hour is more than specified value
Device ID: Cookie state	Checks the cookie state for the given device and user
Device ID: Cookies match	Tracker node matches for both cookies
Device ID: Header data match	Determines if header data is match
Device ID: Header data match percentage	Determines if header data match percentage is within specified range
Device ID: Header data present	Determines if header data is present
Device ID: Is cookie disabled	Determines if cookie is disabled for the user based on history
Device ID: Is cookie empty	Determines if the cookie value is empty or not empty. Validation check is not included
Device ID: Is cookie from same device	Determines if the HTTP and flash cookies are from the same device. Automatically checks the old nodes if the current node is not found
Device ID: Is cookie old	Determines if the cookie sent is from an old cookie
Device ID: Is cookie valid	Determines if there is a valid node for the given cookie value.

Condition Name	Condition Description
Device ID: HTTP header data browser match	Determines if browser is matched based on HTTP header data
Device ID: HTTP header data browser upgrade	Determines if browser is upgraded based on HTTP header data
Device ID: HTTP header data operating system match	Determines if operating system match based on HTTP header data
Device ID: HTTP header data operating system upgrade	Determines if operating system is upgraded based on HTTP header data. Check is based on versions
Device ID: Known header data match percentage	Determines if the known header data match percentage is within the specified range
User: User ASN first time	Checks to see if the user has used this ASN successfully previously
User: User carrier first time	Checks to see if the user has successfully used this carrier previously
User: User city first time	Checks to see if the user has used this city successfully previously
User: User country first time	Checks to see if the user has used this country successfully previously
User: User IP first time	Checks to see if the user has used this IP successfully previously
User: User ISP first time	Checks to see if the user has used this ISP successfully previously
User: User state first time	Checks to see if the user has used this state successfully previously
Device ID: User used this fingerprint	Checks to see if the user has used this fingerprint previously
Entity: Entity is a member of the pattern bucket for the first time in a certain time period	Condition to find out whether this entity is member of the pattern bucket for the first time in a certain time period
Entity: Entity is a member of the pattern bucket less than some percent with all other entities involved	Checks to see if this entity has been a member of this pattern bucket based on percent basis, taking into account all other entities
Entity: Entity is a member of the pattern less than some percent times	Checks to see if this entity has been a member of this pattern condition based on percent basis
Entity: Entity is a member of the pattern N times	Checks to see if this entity has been a member of this pattern condition
Entity: Entity is a member of the bucket N times in a given time period	Checks to see if this entity has been a member of this bucket. You can compare if this entity has been belonging to this bucket before
Location: ASN in group	Checks to see if the ASN for the current IP address is (or is not) in the ASN group
Location: Domain in group	Checks to see if the second-level domain is in the group
Location: In carrier group	If the IP is in the given carrier group
Location: City in group	If the IP is in the given city group
Location: IP connection speed in group	Checks to see if the IP connection speed is in the group
Location: IP connection type in group	Checks to see if the IP connection type is in the group
Location: IP connection type	The connection type for the IP. The type could be DSL, Cable, ISDN, Dialup, fixed wireless, mobile wireless, satellite, frame relay, T1/T3, OCx, and others

Condition Name	Condition Description
Location: In Country group	If the IP is in the given country group
Location: IP excessive use	If IP is excessively used that has not been used before
Location: IP in group	If the IP is in the IP group
Location: IP in range group	If the IP is in the IP range specified in an IP range group. The condition checks to see if the IP of the activity belongs to one of the IP ranges specified in the list of ranges
Location: IP is AOL	Checks to see if the IP is from AOL Proxy
Location: IP line speed type	The connection line speed type for the IP. This is categorized into High, Medium, Low, or Unknown
Location: IP Maximum logins	Maximum number of logins using the current IP address within the given time duration. This condition ignores the current request during evaluation of the Max logins count
Location: IP Maximum users	Maximum number of users using the current IP address within the given time duration
Location: IP multiple devices	Maximum number of devices from IP address within the given time duration
Location: IP routing type	The routing type for the IP. The type 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 to see if the IP routing type is in the group
Location: IP type	If IP is valid, unknown, or private
Location: ISP in group	Checks to see if the ISP for the current IP address is (or is not) in the ISP group
Location: State in group	If the IP is in the given state group
Location: Timed not status	Maximum login attempts for all but the given status within the given time period
Location: Top-level domain in group	Checks to see if the top-level domain is in the group
Location: User status count	Checks user count with the given status from this location in specified duration
Session: Check parameter value	Checks to see if specified parameter value is more than specified value
Session: Check parameter value for regular expression	Checks to see if specified parameter value matches regular expression
Session: Check parameter value in group	Checks to see if specified parameter value is in group
Session: Check string parameter value	Compares string value
Session: Check two string parameter values	Compares two parameters string values
Session: Check value in comma-separated values	Checks to see if specified value is present in the comma-separated value list
Session: Compare two parameter values	Compares two parameter values
Session: Compare with current date time	Compares specified parameter value with current time

Condition Name	Condition Description
Session: Cookie mismatch	Checks to see if there is a mismatch between the supplied cookie and the expected cookie
Session: IP changed	IP address is changed since transaction is started
Session: Mismatch in browser fingerprint	Checks to see if there is a mismatch between the browser fingerprint and the fingerprint supplied during authentication. The fingerprint is constructed using the context values passed to the rules engine
Session: Time Unit	Checks to see if the current time unit matches the specified time unit criteria
System - Check Boolean Property	Check system property
System - Check Int Property	Check system property
System - Check Model Maximum Score	Checks the model's maximum score
System - Check Model Minimum Score	Checks the model's minimum score
System - Check Request Date	Checks request date
System - Check String Property	Check system property
System - Evaluate Policy	Process the policy as rule and evaluate results
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 if consecutive transactions in given duration satisfy the filter conditions	Checks to see if consecutive transactions in given duration that satisfy the filter conditions
Transaction: Check current transaction using the filter conditions	Checks current transaction using filter conditions
Transaction: Check transaction aggregate and count using filter conditions	Checks transaction aggregate and count using filter conditions
Transaction: Check transaction count using filter conditions	Checks transaction count using filter conditions
Transaction: Check Unique Transaction Entity Count with the specified count	Checks unique transaction entity count with the specified count
Transaction: Compare transaction aggregates (Sum/Avg/Min/Max) across two different durations	Compares transaction aggregates (Sum/Avg/Min/Max) across two different durations
Transaction: Compare transaction counts across two different durations	Compares transaction counts across two different durations
Transaction: Compare transaction entity or element counts across two different durations	Compares transaction entity or element counts across two different durations
User: Account Status	Account status of the user
User: Action Count	Checks action counter for the given action. This condition has a dependency on action configuration

Condition Name	Condition Description
User: Action Count Timed	Checks to see if the given action count is more than the specified count. If runtime is not specified, the action is checked in all runtimes
User: Action Timed	Maximum number of actions in the past x seconds
User: User Agent Percentage Match	Checks to see if user agent percentage match is above specified percentage. Compares with UAS of previous login from same device
User: ASN first time for user	Is the user using this ASN for the first time
User: Authentication image assigned	Checks to see if an authentication image is assigned to the user
User: Authentication Mode	Check user authentication mode
User: Challenge Channel Failure	If a user has a failure counter value more than a specified value from specific channel
User: Challenge Failure	If a user has a failure counter value more than a specified value for more than a specific time
User: Challenge Maximum Failures	Checks to see 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 to see if user answered challenge question successfully in last n days
User: Check first login time	Checks to see if the user first logged in within range. First login is the first successful login
User: Check information	Checks to see if the user information is set. Information data to check is sent as a key value pair
User: Check login time	Checks to see if user login time is within the specified time
User: Check Last Session Action	Checks to see if the given action is in the last session. If runtime is not specified, the action is checked in all runtimes of that session
User: Check login count	Checks user login count within specified duration
User: Check login time	Checks to see if user login time is within the specified time
User: Check OTP failures	Checks to see if user's OTP failure counter value is more than a specified value
User: Check User Data	Checks User Data for the given key
User: City first time for user	Is the user using this city for the first time
User: Client and Status	Account status of the user
User: Country failure count for user	Check failure count for the user from the given country
User: Country first time from list	If this country is used for the first time by this user from the given country list
User: Country first time for user	Is the user using this Country for the first time
User: Devices	Number of devices tried in given time
User: Distance from last successful login	Distance from last successful login within specified time
User: Distance from last successful login within limits	Checks to see if distance from last successful login within specified time is within in limits
User: Image Status	Image status of the user
User: In Group	If the user is in the given group

Condition Name	Condition Description
User: IP carrier first time for user	Is the user using this IP carrier for the first time
User: Is last IP match with current IP	Checks to see if user login IP address matches with that of previous login
User: Is User Agent Match	Checks to see if user agent matches with that of previous login from same device
User: Last login	Last login within specified time
User: Last login status	Checks to see if user login status is in specified list
User: Location Used Timed	If user used this location within the given time period
User: Login first time for user	Checks to see if user is logging in for the first time
User: Login In group	If the user login is in the given group
User: Login time between specified times	Login time between specified time
User: Max Countries	Number of countries within the given time period
User: Max IPs Timed	Max number of IPs within the given time period
User: Max Locations Timed	Max number of locations within the given time period
User: Max Cities	Number of cities within the given time period
User: Max States	Number of states within the given time period
User: Multiple failures	User failed multiple times
User: Phrase Status	Phrase status of the user
User: Preferences Configured	Checks to see if the user preferences are set
User: Question Status	Question status of the user
User: Runtime score	Checks to see if the score is within limits
User: Stale session	Checks to see if there is newer login after current login session is established.
User: State first time for user	Is the user using this State for the first time
User: Status Count Timed	User attempted multiple log ins in specified time
User: User Agent Percentage Match	Checks to see if user agent percentage match is above the specified percentage. Compares with UAS of previous login from same device
User: User Group in List	If the user group is in the given list
User: User is member of pattern N times	Checks to see if this user has been member of this pattern condition
User: Velocity from last successful login	Velocity from last successful login
User: Velocity from last successful login within limits	Triggers when velocity from last successful login is within specified limits

B.1 Descriptions

This chapter focuses on device, autolearning, location, transaction, in-session, system, and user conditions.

B.1.1 Device Conditions

This section provides information on the following device conditions:

- Device: Browser header substring
- Device: Device firsttime for user
- Device: In Group
- Device: Excessive Use
- Device: Is registered
- Device: User count
- Device: Timed not status
- Device: Used count for User
- Device: Velocity from last login

B.1.1.1 Device: Browser header substring

Condition	DEVICE: Browser header substring
Description	Checks whether the supplied string exists as a substring in the browser's header information. The string comparison is performed by ignoring the case (uppercase or lowercase) of the strings.
Pre-Requisites	
Assumptions	The rule is configured through a policy.
Available since version	Pre-10.1.4.5
Checkpoints	All checkpoints.

Parameters

Parameter	Description	Possible Values	Can be Null?
subString	Substring to be checked with the string present in the browser.		Yes

Possible User Scenarios

This condition could potentially be used to determine if the user is logging in from a particular version of a browser that is prone to security problems.

B.1.1.2 Device: Device firsttime for user

Condition	DEVICE: Device firsttime 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.
Pre-Requisites	The rule should be configured through a policy.
Assumptions	
Available since version	Pre-10.1.4.5

Condition	DEVICE: Device firsttime for user
Checkpoints	All checkpoints.

Parameters

Parameter	Description	Possible Values	Can be Null?
is	Boolean that checks if the condition should return true or false if the user is using this device for the first time	true (default) or false	Cannot be Null.

Possible User Scenarios

This condition 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.

B.1.1.3 Device: In Group

Condition	DEVICE: In Group
Description	Checks to see if the device is in the specified list.
Pre-Requisites	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

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

Possible User Scenarios

This condition can be potentially used to determine if the device of the current activity belongs to a particular list of devices.

For example,

- You may 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.

B.1.1.4 Device: Excessive Use

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.
Pre-Requisites	You should have this rule configured through a policy.
Assumptions	
Available since version	10.1.4.5
Checkpoints	All checkpoints.

Parameters

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

Possible User Scenarios

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.

B.1.1.5 Device: Is registered

Condition	DEVICE: Is registered
Description	Condition checks to see if the device where that the user is logging in is registered for the user.
Pre-Requisites	You should have this rule configured through a policy.
Assumptions	
Available since version	10.1.4.5
Checkpoints	All checkpoints.

Parameters

Parameter	Description	Possible Values	Can be Null?
is	Boolean parameter to decide if the default return value should be true or false if the device is registered.	[True] / False	Yes

Possible User Scenarios

This condition can be used to identify if the user is 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.

B.1.1.6 Device: User count

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.
Pre-Requisites	You should have this rule configured through a policy.
Assumptions	
Available since version	10.1.4.5
Checkpoints	All checkpoints.

Parameters

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

Possible User Scenarios

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.

B.1.1.7 Device: Timed not status

Condition	DEVICE: Timed not status
Description	This condition counts the attempts by users from the same device (the device 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.
Pre-Requisites	You should have this rule configured through a policy.
Assumptions	
Available since version	10.1.4.5
Checkpoints	All checkpoints.

Parameters

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
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

Possible User Scenarios

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.

B.1.1.8 Device: Used count for User

Condition	DEVICE: Timed not status
Description	This condition counts the attempts by users from the same device (the device 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.
Pre-Requisites	You should have this rule configured through a policy.
Assumptions	
Available since version	10.1.4.5
Checkpoints	All checkpoints.

Parameters

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

Parameter	Description	Possible Values	Can be Null?
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

Possible User Scenarios

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.

B.1.1.9 Device: Velocity from last login

Condition	DEVICE: Velocity from last 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 highly dependent on the accuracy of the location data.
Pre-Requisites	This rule is configured through a policy. Location database should be loaded for the rule. You might also need tools (like a browser header modifier plug-in) to simulate the different IP for the incoming session.
Assumptions	Location database is loaded.
Available since version	10.1.4.5
Checkpoints	All checkpoints.

Parameters

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 user has traveled faster than this value, then condition will evaluate to true.	positive integer (default = 60)	No
sinceSeconds	This is a parameter that is a positive integer that specifies the time difference between this login and last login to calculate user's velocity.	positive integer (default = 172800 which is 48 hours)	No

Possible User Scenarios

This condition can be used to determine the users's 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 login.

One of the simplest scene is when the user is 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 login (use default values).

Another case involves users traveling on air transport. You can use different values (for example, 500 miles an hour) to make sure that login locations and speed are within reason.

However, be aware that the velocity calculation depends highly on location databases.

B.1.2 Autolearning Conditions

The section provides information on the following autolearning conditions:

- Entity: Entity is Member of Pattern Bucket for the first time in Certain Time Period
- Entity: Entity is member of pattern less than some percent times
- Entity: Entity is member of pattern bucket less than some percent with all entities in picture
- Entity: Entity is member of pattern N times
- Entity: Entity is member of bucket N times in a given time period

B.1.2.1 Entity: Entity is Member of Pattern Bucket for the first time in Certain Time Period

Condition	Entity: Entity is Member of Pattern Bucket for the first time in Certain Time Period
Description	Condition to find out 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."
Pre-Requisites	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

Parameter	Description	Possible Values	Can be Null?
Pattern Name	Name of the pattern for which the "first time" bucket is to be checked.		Cannot be null.
Is	Evaluate this condition to true if this parameter is true and "first time" bucket is true.		Cannot be null
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)	Cannot be null.

Parameter	Description	Possible Values	Can be Null?
Time period for bucket membership	The time period over which the pattern membership is evaluated. The units of time	Positive number. (Use numbers that would be valid for the time period type). Use 0..24 for hours, use 1 through 12 for months, 1 through 31 for days, and 1 through 8 for years.	Cannot be null
Member type for pattern-bucket membership	The member type (user, device, location, city, country)	Type for members applicable for that transaction. For authentication type it is one of user, device, IP, city, state, country.	Cannot be null.
First time count	The count of occurrences 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)	Cannot be null

Possible User Scenarios

Examples of how to use this condition are:

- To develop first time rules. For example, define a user (city for each) pattern and attach this pattern to this condition-based rule in a policy, so that when the user logs in from a city the first time, the rule will be triggered.
- To challenge users when they are performing an action for the first time in transactions. For example user tried to perform a bill transfer of 5000 dollars. This can be achieved using a pattern that has user and the transaction amount ranges 1..100, 1000...10000 and so on.

B.1.2.2 Entity: Entity is member of pattern less than some percent times

Condition	Entity: Entity is member of pattern less than some percent times
Description	Condition to find out whether this entity is member of the pattern bucket for less than a certain percent in a certain time period. This condition checks the pattern membership percentage against the pattern usage of the same entity. With this condition, the entity's membership count for percentage is counted and not the number of entities that belong to that pattern.
Pre-Requisites	You should have entities and patterns defined before you try to add this to rule / policy.
Assumptions	Autolearning is enabled.
Available since version	10.1.4.5
Checkpoints	All checkpoints

Parameters

Parameter	Description	Possible Values	Can be Null?
Pattern Hit Percent less than	Percent hit count of the pattern that will be used for comparison	Make sure you pass "good" values. Providing values in decimal points is not recommended since the percentage values may be a Double type of values when calculated over a large number of login and pattern usage combination. For example, do not enter 10.45362. Instead enter 10.5 or 10 or 11.	Cannot be null
Pattern name for membership	Name of the pattern for which the membership count is to be checked.		Cannot be null
Is Membership Count Less than patternHitPercent	Evaluate this condition to true if this parameter is true and the pattern percent is less than the given value		Cannot be null
Time period type for pattern membership	The time period type (hours, days, months of years)	One of wotk.type.enum. That is (hour, day, month, year)	Cannot be null.
Time period for pattern membership	The time period over which the pattern membership is to be evaluated; the units of time	Positive number. (Use valid numbers depending on time period type). Use 0..24 for hours, use 1 through 12 for months, 1 through 31 for days, and 1 through 8 for years.	Cannot be null
Member type for pattern 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.	Cannot be null.

Possible User Scenarios

This can be most effectively used in tracking the user's habits. For example, if the user usually logs in from a certain state and he starts logging in from other states also. In that case, he will be challenged on the first few times he logs in from those states since the percentage for those state will be lower than 10% (if 10 was entered as the Pattern Hit Percent less than). User (for each state) pattern can created for use in tracking the user's logins from different cities.

B.1.2.3 Entity: Entity is member of pattern bucket less than some percent with all entities in picture

Condition	ENTITY: Entity is member of pattern bucket less than some percent with all entities in picture
Description	<p>Condition to find out 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.</p> <p>This condition considers all the other entities; therefore performance is affected more than for simpler conditions.</p>

Condition	ENTITY: Entity is member of pattern bucket less than some percent with all entities in picture
Pre-Requisites	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

Parameter	Description	Possible Values	Can be Null?
Pattern bucket hit percent less than	Percent hit count of the pattern that will be used for comparison	Try to use a sensible number. Use 10 or 11 in place of 10.7623591 as an example.	Cannot be null
Pattern name for membership	Name of the pattern for which bucket percentage is checked.		Cannot be null.
Is Membership Count Less than patternHitPercent	Evaluate this condition to true if this parameter is true and percentage is less than the specified percentage.		Cannot be null
Time period type for pattern membership	The time period type (hours, days, months of years)	One of wotk.type.enum. That is (hour, day, month, year)	Cannot be null.
Time period for pattern membership	The time period over which the pattern membership is to be evaluated. Units of time.	positive number. (Use valid numbers for the time period type). Use 0..24 for hours, use 1 through 12 for months, 1 through 31 for days, and 1 through 8 for years.	Cannot be null
Member type for pattern 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.	Cannot be null.

Possible User Scenarios

This condition can be used to find out whether users are performing actions that are not consistent with the action of other users. For example, a user is logging in from a city that most users do not log in from usually.

Non-popular states, cities, IPs, and others can be enforced using these condition.

B.1.2.4 Entity: Entity is member of pattern N times

Condition	ENTITY: Entity is member of pattern N times
Description	Condition to find out whether this entity is a member of the pattern "n" number of times.
Pre-Requisites	You should have entities and patterns defined before you try to add this to rule / policy.
Assumptions	Autolearning is enabled.

Condition	ENTITY: Entity is member of pattern N times
Available since version	10.1.4.5
Checkpoints	All checkpoints.

Parameters

Parameter	Description	Possible Values	Can be Null?
Pattern hit count more than	Hit count of the pattern that will be used for comparison. If hit count for the pattern is more than this value, then the condition returns true.	For Pre-Authentication execution, set the count one less than what you want the rule to trigger on.	Cannot be null
Pattern name for membership	Name of the pattern for which the membership count is to be checked.		Cannot be null.
Is Membership Count More than patternHitCountFor User	Boolean value that is used to return true or false from the condition. It works as follows: if (isMoreThan == true) and (hitCountMorethan returned true) then condition evaluates to true. ELSE if (isMoreThan == false) and (hitCountMorethan returned false) then condition evaluates to false. and condition evaluates to false in all other cases.		Cannot be null
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)	Cannot be null
Time period for pattern membership	The time period over which the pattern membership is evaluated. Units of time	positive number. (Specify valid values for the time period type). Use 0 through 24 for hours, 1 through 12 for months, 1 through 31 for days, and 1 through 8 for years.	Cannot be null
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.	Cannot be null.

Possible User Scenarios

Condition can be used to find out whether the user has performed a particular operation a few times and the operation is well defined. For example if user logged in from a group of IP that are tagged as anonymizer. If user logs in like that a few times, a policy can be configured to take an action.

B.1.2.5 Entity: Entity is member of bucket N times in a given time period

Condition	ENTITY: Entity is member of bucket N times in a given time period
Description	Condition to find out whether this entity has been a member of the bucket several times in a given time period. This condition can be used to check the current behavior against the pattern. Note that this is a count-based condition. So, if you configure to trigger it, for example, for a count less than three, it will trigger on the first login that matches the pattern.
Pre-Requisites	Ensure that the following pre-requisites are met: <ul style="list-style-type: none"> 10.1.4.5.2 or later must be installed. 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

Parameter	Description	Possible Values	Can be Null?
Pattern name for membership	Name of the pattern for which the bucket membership is to be checked. In the Rule's Condition tab, select the pattern from a drop-down of active patterns that will be presented.		Cannot be null.
Time period for bucket membership	The time period over which the bucket membership is to be evaluated. This is in units of time.	Use 1 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.	Cannot be null
Time period type for bucket membership	The time period Type (hours, days, months of years)	One of workflow.type.enum. That is (hour, day, month, year)	Cannot be null
Member type for pattern membership	The member Type (user, device, location [city, state, country], IP)	It is one of the type of members applicable for that transaction. For authentication type it is one of user, device, IP, city, state, country.	Cannot be null
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 Entity: Entity is member of bucket 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.	Cannot be null

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.operat or.enum equal_to not_equal_to less_than less_than_or_equal_to more_than more_than_or_equal_to are the possible values.	Cannot be null.
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	Cannot be null
Return value if condition encounters an error	This is the value that will be returned if the condition execution runs into issue. Some possible errors: 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	Cannot be null.

Possible User Scenarios

This condition can be used to find out whether the user performed a particular operation a few times that was well defined. For example, if a user logged in from a city for a few times, the information can be used to challenge the user for the first few times.

B.1.3 Location Conditions

This section provides information on the following location conditions:

- [Location: ASN in group](#)
- [Location: IP in Range group](#)
- [Location: In Country group](#)
- [Location: IP Connection type in group](#)
- [Location: IP line speed type](#)
- [Location: IP Routing Type in group](#)
- [Location: In carrier group](#)
- [Location: IP Maximum Users](#)
- [Location: Is IP from AOL](#)
- [Location: in city group](#)

B.1.3.1 Location: ASN in group

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.
Pre-Requisites	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

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

Possible User Scenarios

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.

B.1.3.2 Location: IP in Range group

Condition	LOCATION: IP in Range group
Description	Checks whether the IP of the current activity belongs to a list of IP-ranges specified.
Pre-Requisites	There should a group defined already which has IP-ranges as members. You should have this rule configured through a policy.
Assumptions	
Available since version	10.1.4.5.1
Checkpoints	All checkpoints.

Parameters

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

Possible User Scenarios

This condition can be potentially used to determine if the IP of the current activity belongs to one of several ranges of IPs that may be of interest. For example you might have ranges of IPs from a particular subnet and you might want to take action if that is the case.

B.1.3.3 Location: In Country group

Condition	LOCATION: In Country group
Description	Checks whether the IP belongs to a given country group.
Pre-Requisites	There should a group defined already which has countries as members. You should have this rule configured using some model. IP location data is useful for this condition. (Most production environments will have application database populated)
Assumptions	
Available since version	
Checkpoints	All Checkpoints.

Parameters

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. Use the Group editor in OAAM Admin to edit the group.	(java Long values)	Yes

Possible User Scenarios

This condition can be potentially used to find out 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.

B.1.3.4 Location: IP Connection type in group

Condition	LOCATION: IP Connection type in group
Description	Find out whether the connection type of this IP location is in the group of connection types that might be of interest.
Pre-Requisites	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

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.
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

Possible User Scenarios

This condition can be used to find out 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."

B.1.3.5 Location: IP line speed type

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
Pre-Requisites	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

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.

Parameter	Description	Possible Values	Can be Null?
speed type	This is the enumeration value that indicates connection speed type. This (connection speed) is categorized into High, Medium, Low or Unknown The enum that is used for this parameter is location.linespeed.enum	(Integer) Default value is location.linespeed.enum.low	Yes

Possible User Scenarios

This condition can be used potentially to find out 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.

B.1.3.6 Location: IP Routing Type in group

Condition	LOCATION: IP Routing Type in group
Description	Checks to see if the IP Routing Type is in the group.
Pre-Requisites	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

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

Possible User Scenarios

This condition can be potentially used to find out 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.

B.1.3.7 Location: In carrier group

Condition	LOCATION: Carrier in group
Description	Checks to see if the IP is in the given carrier group
Pre-Requisites	There should a list of carriers already defined. You should have this rule configured using a policy. Location data is helpful for the condition.

Condition LOCATION: Carrier in group

Assumptions

Available since version

Checkpoints All checkpoints.

Parameters

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 to edit carrier group.		Yes

Possible User Scenarios

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.

B.1.3.8 Location: IP Maximum Users

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.

Pre-Requisites You should have this rule configured using a policy.

Assumptions

Available since version

Checkpoints All Checkpoints.

Parameters

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 = 300]	No
The maximum number of users	Maximum number of users allowed.	integer [Default = 5]	No

Possible User Scenarios

This condition can be used to find out if a particular IP is being used by fraudsters to perform logins / transactions by using different login IDs they have stolen. In such

cases you will see a number of different logins from the same IP during a relatively short period.

B.1.3.9 Location: Is IP from AOL

Condition	LOCATION: Is IP from AOL
Description	Find out whether the IP is from AOL proxy
Pre-Requisites	You should have this rule configured using a policy to test it.
Assumptions	
Available since version	
Checkpoints	All checkpoints.

Parameters

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

Possible User Scenarios

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.

B.1.3.10 Location: in city group

Condition	LOCATION: in city group
Description	Checks whether the current activity belongs to a given city group.
Pre-Requisites	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

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 admin user interface to edit this group list.	(java Long values)	Yes

Possible User Scenarios

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.

B.1.4 Transactions Conditions

This section provides information on the following transaction conditions:

- [Transaction: Check Current Transaction Using Filter Condition](#)
- [Transaction: Check Transaction Count Using Filter Condition](#)
- [Transaction: Check Transaction Aggregate and Count Using Filter Conditions](#)
- [Transaction: Check Count of any entity or element of a Transaction using filter conditions](#)
- [Transaction: Check if consecutive Transactions in given duration satisfy the filter conditions](#)
- [Transaction: Compare Transaction Aggregates \(Sum/ Avg/Min/Max\) across two different durations](#)
- [Transaction: Compare Transaction counts across two different durations](#)
- [Transaction: Compare Transaction Entity/Element counts across two different durations](#)

Note: The filter operators "like" and "not like" work only on transaction data and entity data where the data type is string.

B.1.4.1 Transaction: Check Current Transaction Using Filter Condition

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.
Pre-Requisites	<ol style="list-style-type: none"> 1. Transactions should be defined. 2. Transaction type of the current transaction should be the same as the transaction type specified in the rule condition
Assumptions	If there are multiple transactions in the current session, then this condition is applied on the last transaction
Available since version	10.1.4.5.1
Checkpoints	All checkpoints.

Parameters

Parameter	Description	Possible Values	Can be Null?
trxDefKey	Transaction type of the transaction to be counted. It represents the Transaction Definition fully qualified key. This is specified using the list box that has the list of transaction definitions		No
filter1Key	These parameters specify the left hand side of the filter conditions. The left hand side represents the fully qualified key of the transaction field. This field could be an entity field or data field or transaction attribute or request attribute.		Yes
filter2Key			
filter3Key			
filter4Key			
filter5Key			
filter6Key			
filter1Condition	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.		Wherever the filterKey is specified, an appropriate condition has to be specified
filter2Condition	The right hand side is the value, which could be a simple value, the value of the current transaction, or a group. <ul style="list-style-type: none"> ■ Value: A simple value that is entered into a field ■ Current: A value from the current transaction. A value is selected from a list of values based on the current entities. ■ Group: Group is automatically selected if you chose the condition as IN or NOT IN. After Group is selected, you will have to select a type of group. Then, based on type, a list box appears with other values to select from, and so on. 		
filter3Condition			
filter4Condition			
filter5Condition			
filter6Condition			

Possible User Scenarios

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).

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.

B.1.4.2 Transaction: Check Transaction Count Using Filter Condition

Condition	TRANSACTION: Check Transaction Count Using Filter
Description	Check the transaction count with a specified value. You can specify the criteria for the transaction to be counted using the filter conditions (up to 6 conditions) and you can also specify the other parameters like the duration to be considered and the transaction status to consider etc.
Pre-Requisites	<ul style="list-style-type: none"> ■ Transactions should be defined. ■ Transaction type of the current transaction should be same as the transaction type specified in the rule condition
Assumptions	If there are multiple transactions in the current session, then this condition is applied on the last transaction
Available since version	10.1.4.5.1
Checkpoints	All checkpoints.

Parameters

Parameter	Description	Possible Values	Can be Null?
trxDefKey	Transaction type of the transaction to be counted. It represents the Transaction Definition fully qualified key. This is specified using the list box that has the list of transaction definitions		No
specifiedConditionEnumForCount	Operator to be applied for the count condition. Specify greater than, greater than or equals, less than, less than or equals		No
specifiedValueForCount	Transaction count numeric value to check		No

Parameter	Description	Possible Values	Can be Null?
durationDescriptor	<p>Specify the duration during which the transactions have to be counted. The duration descriptor enables you to specify the duration.</p> <p>Important: By default, durationType is "rolling," meaning it takes the current time as the end point to count backward to the start point.</p> <p>Whenever the duration is described as "last" x seconds/minutes/hours/days, the rolling type duration has to be used.</p> <p>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.</p> <p>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".</p> <p>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.</p> <p>Examples of "rolling" and "calendar":</p> <p>A "calendar" week starts from Sunday regardless of the current day, whereas the "rolling" week starts from 7 days from the current day.</p> <p>A "calendar" month starts from the 1st of the current month, whereas the "rolling" month starts from the same day of the previous month.</p> <p>A "calendar" year starts from January 1st of the current year, whereas the "rolling" year starts from the same day of the previous year.</p> <p>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.</p> <p>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.</p>		No

Parameter	Description	Possible Values	Can be Null?
transactionStatusEnum	Specify the transaction status that has to be considered for counting. Do not specify any status if you want to consider all transactions regardless of their status.		Yes
ignoreCurrentTransactionInCount	Specify if you want to ignore the current transaction (if any) in the count. If there are multiple transactions and if this is specified as true, only the last transaction is ignored.		Yes
applyFilterOnCurrentTransaction	Specify if you want to check the filter conditions on the current transaction before performing the count. If the filter conditions fail on the current transaction, then the rule condition is evaluated to false without performing the count.		
filter1Key filter2Key filter3Key filter4Key filter5Key filter6Key	These parameters specify the left hand side of the filter conditions. The left hand side represents the fully qualified key of the transaction field. This field could be an entity field or data field or transaction attribute or request attribute.		Yes
filter1Condition filter2Condition filter3Condition filter4Condition filter5Condition filter6Condition	These parameters represent the operator and right hand side of the filter condition. The operator and the right hand side represent the fully qualified key of the filter condition. The right hand side is the value, which could be a simple value, the value of the current transaction, or a group. <ul style="list-style-type: none"> ▪ Value: A simple value that is entered into a field ▪ Current: A value from the current transaction. A value is selected from a list of values based on the current entities. ▪ Group: Group is automatically selected if you chose the condition as IN or NOT IN. After Group is selected, you will have to select a type of group. Then, based on type, a list box appears with other values to select from, and so on. 		Wherever the filterKey is specified, appropriate condition has to be specified

Possible User Scenarios

This condition can be used whenever you want to trigger 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.

B.1.4.3 Transaction: Check Transaction Aggregate and Count Using Filter Conditions

Condition	TRANSACTION: CheckTransactionAggregateAndCountUsingFilter.xml
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 etc.
Pre-Requisites	Transactions should be defined. Transaction type of the current transaction should be same as the transaction type specified in the rule condition
Assumptions	Aggregate 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
Checkpoints	All checkpoints.

Parameters

Parameter	Description	Possible Values	Can be Null?
aggregateFunctionEnum	Aggregate function to check. Available functions are sum, min, max, avg		
elementDefFQKey	Numeric element on which aggregate 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

Parameter	Description	Possible Values	Can be Null?
specifiedConditionEnumForAggregate	Operator to be applied for the aggregate condition. Specify greater than, greater than or equals, less than, less than or equals		No
specifiedValueForAggregate	Aggregate 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	<p>Specify the duration during which the transactions have to be counted. The duration descriptor enables you to specify the duration.</p> <p>Important: By default, durationType is "rolling," meaning it takes the current time as the end point to count backward to the start point.</p> <p>Whenever the duration is described as "last" x seconds/minutes/hours/days, the rolling type duration has to be used.</p> <p>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.</p> <p>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".</p> <p>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.</p> <p>Examples of "rolling" and "calendar":</p> <p>A "calendar" week starts from Sunday regardless of the current day, whereas the "rolling" week starts from 7 days from the current day.</p> <p>A "calendar" month starts from the 1st of the current month, whereas the "rolling" month starts from the same day of the previous month.</p> <p>A "calendar" year starts from January 1st of the current year, whereas the "rolling" year starts from the same day of the previous year.</p> <p>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.</p> <p>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.</p>		No

Parameter	Description	Possible Values	Can be Null?
transactionStatusEnum	Specify the transaction status that has to be considered for counting. If you want to consider all transactions regardless of their status, do not specify any status		Yes
ignoreCurrentTransactionInCount	Specify if you want to ignore current transaction (if any) in the count. If there are multiple transactions and if this is specified as true, only the last transaction is ignored.		Yes
applyFilterOnCurrentTransaction	Specify if you want to check the filter conditions on the current transaction before performing the count. If the filter conditions fail on the current transaction then the rule condition is evaluated to false without performing the count.		
filter1Key filter2Key filter3Key filter4Key filter5Key filter6Key	These parameters specify the left hand side of the filter conditions. The left hand side represents the fully qualified key of the transaction field. This field could be an entity field or data field or transaction attribute or request attribute.		
filter1Condition filter2Condition filter3Condition filter4Condition filter5Condition filter6Condition	These parameters represent the operator and right hand side of the filter condition. The operator and the right hand side represent the fully qualified key of the filter condition. The right hand side is the value, which could be a simple value, the value of the current transaction, or a group. <ul style="list-style-type: none"> ■ Value: A simple value that is entered into a field ■ Current: A value from the current transaction. A value is selected from a list of values based on the current entities. ■ Group: Group is automatically selected if you chose the condition as IN or NOT IN. After Group is selected, you will have to select a type of group. Then, based on type, a list box appears with other values to select from, and so on. 		Wherever the filterKey is specified, appropriate condition has to be specified

Possible User Scenarios

This condition can be used whenever you want to trigger a rule based on 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 aggregate 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 Aggregate condition as "Average."
2. Specify Aggregate 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

B.1.4.4 Transaction: Check Count of any entity or element of a Transaction using filter conditions

Condition	TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions
Condition	TRANSACTION: Check Count of any entity or element of a Transaction using filter conditions
Description	Check to see 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.
Pre-Requisites	Ensure that you are using 10.1.4.5.2 or later. Transactions should be defined; Transaction type of the current transaction should be same as the transaction type specified in the rule condition
Assumptions	
Available since version	10.1.4.5.2
Checkpoints	All checkpoints.

Parameters

Parameter	Description	Possible Values	Can be Null?
trxDefKey	Transaction Definition fully qualified key. This is specified using list box that has list of transaction definitions		No
elementDefFQKey	Transaction Entity/Element that must be counted for checking		No
durationDescriptor	Duration Descriptor		No

Parameter	Description	Possible Values	Can be Null?
forTheSameCurrentUserId	Boolean flag to indicate whether only transactions belonging to the current user to be counted or not		Yes
ignoreCurrentTransactionInCount	Flag to indicate if the current transaction has to be ignored in the count		
specifiedConditionEnumForCount	Condition for the count check. Select only valid operators that are relevant to numeric values		No
specifiedValueForCount	Count value to check. Specify only valid positive integers.		No
applyFilterOnCurrentTransaction	Flag to indicate if the filter conditions have to be validated on current transaction before doing the count		No
filter1Key	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
filter2Key			
filter3Key			
filter4Key			
filter5Key			
filter6Key			
filter1Condition	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
filter2Condition			
filter3Condition			
filter4Condition			
filter5Condition			
filter6Condition			

Possible User Scenarios

This condition can be used whenever you want to trigger a rule based on the count of an entity or entity / data element of the transaction.

For example, you have configured a transaction called "purchase" and you want to trigger a rule if the same user is trying to use more than 5 different credit cards in the last 2 hours and the amount of purchase is more than \$100.

To achieve this:

1. Select the "Credit Card" "Entity" name as the one to be counted, so that the rule counts the distinct number of credit cards used.
2. Then, select "For the same current user" flag as true.
3. Then, select the duration as 2 rolling hours and 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.

B.1.4.5 Transaction: Check if consecutive Transactions in given duration satisfy the filter conditions

TRANSACTION: Check if consecutive Transactions in given duration satisfy the filter conditions	
Condition	
Description	Check to see whether consecutive transactions in a given duration satisfy the specified filter conditions
Pre-Requisites	<ul style="list-style-type: none"> ■ 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

Parameter	Description	Possible Values	Can be Null?
trxDefKey	Transaction Definition fully qualified key. This is specified using list box that has list of transaction definitions		No
durationDescriptor	Duration Descriptor		No
transactionStatusGroupId	Group of Transaction Statuses that should be considered. If no group is specified then Transaction Status is ignored in the query.		Yes
ignoreCurrentTransactionInQuery	Flag to indicate if the current transaction has to be ignored		
forTheSameCurrentUserId	Flag to indicate if only transactions belonging to the current user to be counted. If this flag is false then transactions irrespective of users will be considered.		No
allowGapsForChecks	Flag to indicate if gaps are allowed while checking for conditions. If this value is TRUE then gaps would be allowed while checking for conditions.		No
noOfTransactionsToCheckFor1stCheck	Number of transactions that should satisfy the 1st check. Specify positive integers.		No

Parameter	Description	Possible Values	Can be Null?
filter101Key	Filter Keys for 1st check.		Yes
filter102Key	<p>These parameters specify the left hand side of the filter conditions. It represents fully qualified key of the transaction field.</p> <p>This field could be an entity field or data field or transaction attribute or request attribute.</p> <p>Note: There is a widget for this that renders list box with all the data fields.</p>		
filter103Key			
filter104Key			
filter105Key			
filter106Key			
filter101Condition			
filter102Condition	These parameters represent the operator and right hand side of the filter condition. It represents fully qualified key of the filter condition.		
filter103Condition	<p>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.</p>		
filter104Condition			
filter105Condition			
filter106Condition			
noOfTransactionsToCheckFor2ndCheck	Number of transactions that should satisfy the 2nd check. Specify positive integers.		No
filter201Key	Filter Keys for 2nd check.		
filter202Key	<p>These parameters specify the left hand side of the filter conditions. It represents fully qualified key of the transaction field.</p> <p>This field could be an entity field or data field or transaction attribute or request attribute.</p> <p>Note: There is a widget for this that renders list box with all the data fields.</p>		
filter203Key			
filter204Key			
filter205Key			
filter206Key			
filter201Condition			
filter202Condition	These parameters represent the operator and right hand side of the filter condition. It represents fully qualified key of the filter condition.		
filter203Condition	<p>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.</p>		
filter204Condition			
filter205Condition			
filter206Condition			

Possible User Scenarios

This condition can be used whenever you want to trigger a rule based on checks that are satisfied on consecutive transactions in a given duration.

For example, you have configured a transaction called purchase and you want to trigger a rule if the current/last transaction amount 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.

B.1.4.6 Transaction: Compare Transaction Aggregates (Sum/Avg/Min/Max) across two different durations

TRANSACTION: Compare Transaction Aggregates (Sum/Avg/Min/Max) across two different durations	
Condition	
Description	Compare transactions aggregates across two different durations
Pre-Requisites	<ul style="list-style-type: none"> ■ Transactions should be defined ■ Transaction entity/data field that has to be aggregated should be of type numeric ■ Transaction type of the current transaction should be same as the transaction type specified in the rule condition ■ Ensure that you are using 10.1.4.5.2 or later.
Assumptions	
Available since version	10.1.4.5.2
Checkpoints	All checkpoints.

Parameters

Parameter	Description	Possible Values	Can be Null?
trxDefKey	Transaction Definition fully qualified key. This is specified using list box that has list of transaction definitions		No
aggregateFunctionEnum	Aggregate function that has to be used		No
elementDefFQKey	Transaction Entity/Data Element that must be aggregated		No
durationDescriptorFor1stDuration	Select duration for the first aggregate		No
durationDescriptorFor2ndDuration	Select duration for the second aggregate		No
comparisonConditionEnum	Comparison condition		No

Parameter	Description	Possible Values	Can be Null?
multiplierFor2ndDurationValue	Multiplier value for the second aggregate. 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

Possible User Scenarios

This condition can be used whenever you want to trigger a rule based on the comparison of aggregates of a transaction entity/data element across two different durations.

For example, you have configured a transaction called purchase and you want to trigger if 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 aggregated and "Sum" as the aggregate 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%).

B.1.4.7 Transaction: Compare Transaction counts across two different durations

Condition	TRANSACTION: Compare Transaction counts across two different durations
Description	Compare transactions counts across two different durations
Pre-Requisites	<ul style="list-style-type: none"> ■ 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

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 aggregate. 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 be validated on current transaction before doing the count		No

Parameter	Description	Possible Values	Can be Null?
filter1Key	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
filter2Key			
filter3Key			
filter4Key			
filter5Key			
filter6Key			
filter1Condition	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
filter2Condition			
filter3Condition			
filter4Condition			
filter5Condition			
filter6Condition			

Possible User Scenarios

This condition can be used whenever you want to trigger a rule based on the comparison of transaction counts across two different durations.

For example, you have configured a transaction called "purchase" and you want to trigger if the number of transactions for the current day is 20% more than the number of all transactions of the previous day for that user.

To achieve this:

1. Select 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%).

B.1.4.8 Transaction: Compare Transaction Entity/Element counts across two different durations

Condition	TRANSACTION: Compare Transaction Entity/Element counts across two different durations
Description	Compare transaction entity/element counts across two different durations
Pre-Requisites	<ul style="list-style-type: none"> ■ 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

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 aggregate. 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 be validated on current transaction before doing the count		No
filter1Key	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
filter2Key			
filter3Key			
filter4Key			
filter5Key			
filter6Key			
filter1Condition	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
filter2Condition			
filter3Condition			
filter4Condition			
filter5Condition			
filter6Condition			

Possible User Scenarios

This condition can be used whenever you want to trigger a rule based on the comparison of any transaction entity/element counts across two different durations.

For example, you have configured a transaction called "purchase" and you want to trigger if the number of distinct credit cards used in the current day is 20% more than the number of distinct credit cards used on the previous day for that user.

To achieve this:

1. Select "Credit card" as the element to be counted and select 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%).

B.1.5 In-Session Conditions

The following in-session conditions are documented in this section:

- [Session: Check Param Value](#)
- [Session: Check param value for regex](#)
- [Session: Check param value in group](#)
- [Session: Check String Value](#)
- [Session: Time Unit Condition](#)

B.1.5.1 Session: Check Param Value

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 find out 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.
Pre-Requisites	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.

B.1.5.1.1 Parameters

Parameter	Description	Possible Values	Can be Null?
Is	<p>If the "Is" is true and the value is above the threshold provided then condition evaluates to true.</p> <p>If the "Is" is false and the value is below the threshold provided then condition evaluates to true.</p>	[True] / False	No

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 "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. A string that can be parsed into a number. (all numeric characters and "+", "-" and "." Also time can be used here in "HH24:MM:SS:MS" format. This can be used to see if the time is greater than the time parameter present in the transaction.		Yes

B.1.5.1.2 Possible User Scenarios This condition can be used whenever you want to find out whether the value of a particular attribute of the transaction exceeds some threshold.

For example, you have configured a transaction called purchase and you want to trigger a rule whenever the customer purchase exceeds 1000\$ mark.

For achieving this, you must use this rule with this condition.

Configure the "ValueKey" of your transaction = "purchase.orderTotal" assuming that you have such an attribute in your transaction.

Configure "ValueAbove" = "1000". Configure an alert that says "Too Big Purchase"

Process a transaction by providing some total value numbers above 1000 and some below 1000.

Verify that for the ones above 1000 the rule is triggered.

B.1.5.2 Session: Check param value for regex

Condition	Session: Check param value for regex
Description	Find out whether the specified parameter value matches regular expression. This condition can be used to find out whether some string value of a particular parameter in the transaction matches some known pattern and then action can be taken accordingly. Basically provided some mathematical function for integrators. This will be very useful in native integration.

Condition	Session: Check param value for regex
Pre-Requisites	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.

B.1.5.2.1 Parameters

Parameter	Description	Possible Values	Can be Null?
Is	<p>If the "Is" is true and regular expression matches to the provided criteria then condition evaluates to true.</p> <p>If the "Is" is false and regular expression does not match to the provided criteria then condition evaluates to true.</p>	[True] / False	No
ValueKey	<p>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.</p>		Yes
Regular Expression	<p>The character pattern with which you want to match the "value" whose look up name is given by "ValueKey". In same credit card example. We want to check to see whether the user entered all correct in credit card so we might look for pattern "[0-9]".</p>		Yes
Error Return value	<p>If there is any error then return (evaluate to) this value. If this value is not specified (null) then "False" is assumed.</p>	[False] / True	Yes

B.1.5.2.2 Possible User Scenarios This condition can be used whenever you want to find out whether the value of a particular attribute of the transaction matches some character pattern.

For example, you have configured a transaction called "purchase" and you 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 achieving this, you must use this rule with this condition.

Configure the "ValueKey" of your transaction = "customer.email" assuming that you have such a attribute in your transaction.

Configure "Regular Expression" = "*[.gov][.mil]". Configure an alert that says "Goventment/Military business."

Process some transaction by providing some email address ending with ".gov" or ".mil". Verify that the alert is generated.

Process some transactions by giving another email address ending ".com" or any ending other than ".gov" or ".mil". Notice that alert is not generated.

B.1.5.3 Session: Check param value in group

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)
Pre-requisites	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

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

Parameter	Description	Possible Value	Can be Null
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 we want to find out whether the bankName equals "SomeBank," we 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

Possible User Scenarios

This condition can be used whenever you want to find out 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 = "Transaction.bankName" (assuming that you have such an attribute in your transaction).
2. Configure "Regular Expression" = "(bank.)". Configure some 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" = true and default return value = false.
6. Process some transaction by providing some bank names that are "bank1" and "bank2", "bank3", and so on. Verify that the alert is generated for "bank1" and "bank2" only.
7. Verify that alerts will also be generated for "BANK1". This is to demonstrate that the regular expression matching is not case-sensitive.

B.1.5.4 Session: Check String Value

Condition	Session: Check string value
Description	<p>Check to see whether the specified parameter value is equal to given character string. This condition can be used to find out whether the value of a particular parameter in the transaction matches an expected string and then action can be taken accordingly. Basically provided some string equality function for integrators. This will be very useful in native integration.</p> <p>Note that comparison is case-sensitive. That is "Good" is not equal to "GOOD".</p>
Pre-Requisites	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.

B.1.5.4.1 Parameters

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

B.1.5.4.2 Possible User Scenarios This condition can be used whenever you want to find out 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.

For achieving this, you must use this rule with this condition:

Configure the "ValueKey" of your transaction = "purchase.creditCardType" assuming that you have such an attribute in your transaction.

Configure "StringValue" = "AMEX". Configure some alert that says "Amex Card Used"

Process some transaction by providing the card type as AMEX and some with other card type.

Verify that for using AMEX the rule is triggered.

B.1.5.5 Session: Time Unit Condition

Table B-1 Day of Week

Condition	Day of Week
Description	<p>Checks to see if time unit in current date matches some 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.</p> <p>This condition uses the request date if available to evaluate the date function requested with the help of parameters.</p> <p>If the request date is not available, then current server date time will be used.</p>
Example	<p>This condition can determine if the day of the week is equal to (or not equal to or ...) Monday or Tuesday and so on.</p> <p>It can also determine if the day of the month matches certain criteria of the day of the month.</p> <p>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.</p>

Parameters

Parameters	Description	Possible Values
Time Unit	<p>Enum</p> <p>What is the time unit you are looking for?</p> <p>The default value is Day Of The Week</p>	<p>Possible values are:</p> <ul style="list-style-type: none"> ■ 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	<p>Enum</p> <p>What comparison you want to make with the time unit.</p> <p>The default value=Equal To</p>	<p>Possible values are:</p> <ul style="list-style-type: none"> ■ 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	<p>String</p> <p>The default value = "" (empty string), that represents integer or string that represents comma separated integers. Example: "1" or "1,2,3,4".</p> <p>The user can use comma-separated values when using IN or NOT in operator.</p> <p>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.</p> <p>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.</p>	<p>Correct values of this parameter for different time units.</p> <ul style="list-style-type: none"> ■ Day Of The week: 1 through 7 (1 = Monday). ■ Day Of the month: 1 through 31 ■ Day of the year: 1 through 366 ■ Month of the year: 0 through 11 (0 = January) ■ Hour of the day: 0 through 23 ■ Week of the Month: 0 through 6 ■ Week of the Year 1 through 53 ■ Year: Positive integer
IS Condition True	<p>Boolean</p> <p>Default value = true</p> <p>This will the return value if the comparison is true.</p>	
Error Return value	<p>Boolean</p> <p>Default value = false</p> <p>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.</p> <p>The days of the weeks are:</p> <ul style="list-style-type: none"> ■ 1 = sunday ■ 2 = monday ■ 3 = tuesday ■ 4 = wednesday ■ 5 = thursday ■ 6 = friday ■ 7 = saturday <p>The week day is 2,3,4,5,6</p> <p>Time Unit = Day of the Week</p> <p>Comparison Operator = "IN"</p> <p>Comparison Value = "1,2,3,4,5"</p> <p>Is Condition True = true</p> <p>Error Return value = "false"</p>	

B.1.6 System Conditions

The following transaction conditions are documented in this section:

- [System - Check Boolean Property](#)

- [System - Check Int Property](#)
- [System - Check String Property](#)
- [System - Check Request Date](#)

B.1.6.1 System - Check Boolean Property

Condition	System - Check Boolean Property
Description	Verify if specified property equals true or false.
Pre-Requisites	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.

B.1.6.1.1 Parameters

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

B.1.6.1.2 Possible User Scenarios This condition can be used whenever you want to find out whether the value of a particular property equals 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 achieving this, you must use this rule with this condition.

Configure the "Property" of this condition = "trigger.sample.rule". Configure the PropertyValue = "true". Configure DefaultValue = "false"

Run authentication of users to see if the rule triggers.

Then, go to property editor and change the value of the property "trigger.sample.rule" to false.

Run authentication of users again and notice that the rule does not trigger.

B.1.6.2 System - Check Int Property

Condition	System - Check Integer Property
Description	Verify if specified property equals expected integer value

Condition	System - Check Integer Property
Pre-Requisites	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

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

This condition can be used whenever you want to find out whether the value of a particular property equals expected integer value.

For example, you have a property "trigger.sample.rule.test.integer" and its value = 25.

You want to trigger some rule based on this property.

For achieving this, you must use this rule with this condition.

Configure the "Property" of this condition = "trigger.sample.rule.test.integer".

Configure the PropertyValue = "25". Configure DefaultValue = "30"

Run some authentication users to see the rule triggers.

Then go to property editor and change the value of the property "trigger.sample.rule.test.integer" to 88.

Run some authentication users again and notice that the rule does not trigger.

B.1.6.3 System - Check String Property

Condition	System - Check String Property
Description	Verify if specified property equals expected string value
Pre-Requisites	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

Condition	System - Check String Property
Checkpoints	All Checkpoints.

Parameters

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

Possible User Scenarios

This condition can be used whenever you want to find out whether the value of a particular property equals expected the string value.

For example, you have a property "trigger.sample.rule.test.string" and its value = "test_string".

You want to trigger a rule based on this property.

For achieving this, you must use this rule with this condition.

Configure the "Property" of this condition = "trigger.sample.rule.test.string". Configure the PropertyValue = "test_string" and configure DefaultValue = "some_other_string"

Run authentication on users to see the rule triggers.

Then go to Property editor and change the value of the property "trigger.sample.rule.test.instringteger" to "completely different string value".

Run authentication of users again and notice that the rule does not trigger.

B.1.6.4 System - Check Request Date

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.
Pre-Requisites	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

Parameter	Description	Possible Value	Can be Null?
Date (MM/dd/yyyy)	The date string which user wants to check the request date against.		No
Is After Request Date	To check to see whether the request date is after the specified date or not after specified date.	[True] / False	Yes

Possible User Scenarios

This condition can be used whenever you want to find out whether the transaction or authentication occurred after a certain date.

For example, you want to direct users to certain other policy after given date, and then you can use this rule.

For achieving this, you must use this rule with this condition.

Configure the "Date" of this condition = "12/22/2009" if you want to trigger rule starting 23rd December of 2009. Configure the "Is After"= "true".

Run some authentication on users. If the date is after 12/22/2009 the rule should trigger.

Then go to the Policy editor and change the date in this condition to a future date.

Run some authentication on the users again and notice that the rule does not trigger.

B.1.7 User Conditions

The following user conditions are documented in this section:

- [User: Check User Data](#)
- [User: Stale Session](#)

B.1.7.1 User: Check User Data

Condition	User: Check User Data
Description	Verify if specified key has any related data for the user
Pre-Requisites	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

Parameter	Description	Possible Value	Can be Null?
User Data Key	The complete name of the key which may have associated data for that user. Consider this a property or a configuration property for only that user.	[Strings] Default= email	Yes

Possible User Scenarios

This condition can be used whenever you want to check to see whether the user has an associated data for the key.

For example, you want to find out whether the user has an email defined in his OTP configuration.

You want to trigger some rule based on whether this email field is defined (non-empty) for the user.

For achieving this, you must use this rule with this condition.

Configure the "User Data Key" of this condition = "user_otpContactInfo_email" (for mobile phone, use key="user_otpContactInfo_mobile").

Use the new out-of-the-box base models that are shipped with 11g. This will force user to register for OTP on first or second login.

Run some authentications with the registered users and you can see the rule triggering when they are registered for the OTP email (or mobile if you have used that as key).

Then go to policy editor and change the value of the key "zoom.some.garbage.that.is.not.supposed.to.exist"

Run some authentication users again and notice that the rule does not trigger. (assumption no such key data exists for this weird looking key)

B.1.7.2 User: Stale Session

Condition	User: Stale Session
Description	Verify if a newer session is established after this session is created
Pre-Requisites	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.

Possible User Scenarios

This condition can be used whenever you want to find out whether the user has established a successful login from another channel while this authentication is in progress.

You want to trigger a rule, or an alert, or a rule and an alert based on that.

To achieve this, you must use this rule with this condition. Configure this rule for the post-authentication checkpoint.

Perform log in (for already the registered user) from one browser window (for example, Firefox) and be in the process where you are shown a password pad.

Then, open another browser (for example, Windows Internet Explorer) and perform another login for the same user and complete the login process. Do not log out yet.

When you come back to the first browser and complete the login, you should see this rule triggered.

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](#)

C.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.

C.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.

C.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.

C.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.

C.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.

C.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.

C.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.

C.8 Users Reports

These reports provide data based on the user information.

Report Name	Description
MultipleDevices	Lists all users that use multiple devices.

Oracle Adaptive Access Manager Properties

This appendix provides essential properties used by Oracle Adaptive Access Manager.

D.1 Properties

Action Override

The Action Override feature is turned off by default. To enable action overrides, set the following property to "true":

```
vccrypt.tracker.rules.allowControlledActions
```

Authenticator Phrase

To customize the phrase in the virtual authentication device, set the following parameter:

```
bharosa.user.noun.list
```

Autolearning

To enable autolearning properties:

Set `vccrypt.tracker.autolearning.use.auth.status.for.analysis` and `vccrypt.tracker.autolearning.use.tran.status.for.analysis` properties to true.

1. Ensure that `vccrypt.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:

- `vccrypt.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.

- `vccrypt.tracker.autolearning.use.tran.status.for.analysis`

This property must be set to true for the transaction-related patterns to work. Transaction related patterns are the one that analyze the transaction related data for autolearning. An example is a pattern that profiles users who are performing wire transfer operations.

3. If the properties do not exist, create them.

Case in Username

If you want the username to be in lowercase, set `bharosa.uio.default.username.case.sensitive` to `false`.

Configurable Actions

To enable the configurable actions feature, set `dynamicactions.enabled` to `true`.

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:

```
customer care.case.expirybehavior.enum.csrcase.behavior = expiry
customer care.case.expirybehavior.enum.csrcase.label = Expired
customer care.case.expirybehavior.enum.csrcase.durationInHrs = 24
customer care.case.expirybehavior.enum.csrcase.resetonaccess = false
```

To disable the "expiry" behavior for CSR cases, modify the following property:

```
customer care.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

Out of box, 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 by default in OAAM Admin, the following property should be set to `true`:

```
vcrypt.reports.scheduler.activate property
```

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.

Out-of-the-box Jobs include Monitor data rollup.

D.2 OTP Properties

OTP Properties and their default values are listed as follows:

Challenge Availability

bharosa.uio.default.challenge.type.enum.ChallengeQuestion.available = true

bharosa.uio.default.challenge.type.enum.ChallengeEmail.available = true

bharosa.uio.default.challenge.type.enum.ChallengeSMS.available = true

Challenge Devices (DeviceKeyPadFull, DeviceKeyPadAlpha, DeviceTextPad, DeviceQuestionPad, DevicePinPad, DeviceHTMLControl)

bharosa.uio.default.ChallengeQuestion.authenticator.device=DeviceQuestionPad

bharosa.uio.default.ChallengeSMS.authenticator.device=DevicePinPad

bharosa.uio.default.ChallengeEmail.authenticator.device=DevicePinPad

Contact Info Inputs Enum

bharosa.uio.default.userinfo.inputs.enum.mobile=0

bharosa.uio.default.userinfo.inputs.enum.mobile.name=Mobile Phone

bharosa.uio.default.userinfo.inputs.enum.mobile.description=Mobile Phone

bharosa.uio.default.userinfo.inputs.enum.mobile.inputname=cellnumber

bharosa.uio.default.userinfo.inputs.enum.mobile.inputtype=text

bharosa.uio.default.userinfo.inputs.enum.mobile.maxlength=15

bharosa.uio.default.userinfo.inputs.enum.mobile.required=true

bharosa.uio.default.userinfo.inputs.enum.mobile.order=1

bharosa.uio.default.userinfo.inputs.enum.mobile.enabled=true

bharosa.uio.default.userinfo.inputs.enum.email=1

bharosa.uio.default.userinfo.inputs.enum.email.name=Email Address

bharosa.uio.default.userinfo.inputs.enum.email.description=Email Address

bharosa.uio.default.userinfo.inputs.enum.email.inputname=email

bharosa.uio.default.userinfo.inputs.enum.email.inputtype=text

bharosa.uio.default.userinfo.inputs.enum.email.maxlength=40

bharosa.uio.default.userinfo.inputs.enum.email.required=true

bharosa.uio.default.userinfo.inputs.enum.email.order=2

bharosa.uio.default.userinfo.inputs.enum.email.enabled=true

Contact info preferences

bharosa.uio.default.userpreferences.userinfo.enabled=false

Contact info registration

bharosa.uio.default.register.userinfo.enabled=false

PIN Generation

bharosa.uio.otp.generate.code.length = 5

bharosa.uio.otp.generate.code.characters = 1234567890

D.3 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
```

The Discovery Process

This appendix shows the modeling process in which high-level requirements are translated into security policies.

It contains the following sections:

- [Discovery Process Overview](#)
- [Example Scenario: Transaction Security](#)
- [Example Scenario: Login Security](#)

E.1 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.2 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.2.1 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.2.2 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.2.3 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.2.4 Outcomes

The outcome required by the problem statement in this case is to generate a single Fraud Alert for the security team.

E.2.5 Translation

In the translation step, the problem statement that was broken down is mapped to the OAAM security policy components.

Table E-1 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.2.6 Alert

The best practice is for every evaluation to have a separate alert message.

E.3 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.3.1 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.3.2 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.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 user (logging in from state(s)), if % of logins < 5% of all his logins from this state in last month, then challenge user."

E.3.4 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 logins to states in the last month.

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-2 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: "Entity: Entity is member of pattern less than some percent times"
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.3.6 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

Globalization Support

This chapter provides information on customizing Oracle Adaptive Access Manager for your locale.

F.1 Supported Languages

Oracle Adaptive Access Manager 11g is translated into 26 languages for OAAM Server and 9 for OAAM Admin. 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-admin locale languages is set in the browser (for example Arabic), 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 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.

F.3 Configuring Language Defaults for Oracle Adaptive Access Manager

The default locales are set in the `client_resource_<locale>.properties` file using the `bharosa.locale.enum`. 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 did not exist, create it.

F.3.2 Example 2

A Brazilian bank wants to set Brazilian Portuguese as the default, but wants to display in OAAM Server in 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.4 Dashboard

To view the Dashboard in the language you want, set your browser's language preference to the appropriate language.

The data viewed in the Dashboard is based on the server's time zone, but information is presented per your browser settings.

F.5 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 6.10, "Customizing English Abbreviations and Equivalences."](#)

The phonetics algorithm is only supported in English.

For information on customization for locales, see [Section 6.11, "Customizing Abbreviations and Equivalences for Locales."](#)

F.6 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.7 Adding Registration Questions

During registration, Oracle Adaptive Access Manager presents customers with question menus. When a customer registers, he or she is required to select one question from each menu. These questions become the customer's "registered questions."

To add questions in Oracle Adaptive Access Manager:

1. Log in to OAAM Admin.
2. In the Navigation tree, double-click **Questions** under KBA. The **Questions Search** page is displayed.
3. 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.

You could also open the **New Questions** page by right-clicking **Questions** under **KBA** in the Navigation tree and selecting **Create** from the context menu that appears.

When the **New Question** page first appears, the default value for the question status is Active.

Question, **Category**, **Status**, and **Locale** are required fields.

4. Pick a locale from the list of locales available.

By default, the **Locale** menu displays English and 27 other default locale languages.

5. Type the new question in the **Question** field.

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."

F.8 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 6.11, "Customizing Abbreviations and Equivalences for Locales."](#)

Setting Up Archive and Purge Procedures

This chapter presents the concepts, prerequisites, policies, and post-process procedures in archiving and purging Oracle Adaptive Access Manager-related data.

The Oracle Adaptive Access Manager-related purging scripts are in the `oaam_db_purging_scripts.zip` file located under `IDM_ORACLE_HOME/oaam/oaam_db_scripts`.

G.1 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.

G.2 Archive Process

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.

G.3 Database Archive and Purge

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.

G.3.1 Archive and Purge Data Classification

Oracle Adaptive Access Manager has different sets of transactional tables that will be archived and purged. These sets are summarized in this subsection. The tables in the transaction table sets are listed in [Section G.3.6, "Archive and Purge Details"](#).

G.3.1.1 Device Fingerprinting

The device fingerprinting data is archived and purged based on the following criteria:

- archive and purge the device fingerprinting logs that are older than a specified period first.
- archive and purge user device maps that are not used after the data from the device fingerprinting logs is purged.

- archive and purge the device history that is not used after the data from the device fingerprinting logs is purged.
- archive and purge the device data that is not used after the data from the device fingerprinting logs is purged.

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.

G.3.1.2 Transaction In-Session Based Data

The in-session transaction data is archived and purged based on the following criteria:

- archive and purge the in-session transactional-based data that is older than a specified period first.
- archive and purge transaction data that is not used in the transaction data after the transactions logs are purged for a specific time period.
- archive and purge the entity, entity profile, user entity map and entity transaction map after the transactions logs are purged for a specific time period.

G.3.1.3 Autolearning Profile Data

The autolearning and profile data is archived and purged based on the following criteria:

- archive and purge the Workflow tables based on a specific time period.
 - 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.

These values are hard-coded. The profile data value can be changed in the execution script for no of days.

- archive and purge fingerprinting data with fingerprint type 11, 12, and no child records in the Workflow tables

```
vcrypt.fingerprint.type.enum.autolearning.auth=11
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.
- archive and purge profile related data that is 183 days old and profiles type 2 (Autolearning Profile) from the autolearning profiles tables.

G.3.1.4 Rule Log Data

The rule log transaction data is archived and purged based on the following criteria:

- archive and purge the rule log data that is 30 days old

G.3.2 Archive and Purge Process

The sections following provide procedures for the archive and purge process.

G.3.2.1 Archive and Purge Process - Special Recommendations for Schemas with Partitioned Objects

This subsection provides special recommendations for schemas with partitioned objects.

G.3.2.1.1 Schema with Partitioned Objects (Oracle Databases Only) Without a Separate Reporting Database If you are using an Oracle Adaptive Access Manager schema with the partition option enabled and do not have a separate reporting and administrative environment, perform only manual purging, as described in this document. Partition drop scripts are part of the partition base package. These scripts are not shipped with the purging scripts.

Follow these steps:

1. Set up archive and purge routines.
2. Schedule archive and purge routines.

G.3.2.1.2 Schema with Partitioned Objects (Oracle Databases Only) With a Separate Reporting Database If you are using an Oracle Adaptive Access Manager schema with the partition option enabled and have a separate reporting and administrative environment, you must perform manual purging, as described, as well as run the partition maintenance scripts that are shipped with the Oracle Adaptive Access Manager database setup package.

Note: Make sure replication is not enable during the archive and purge process.

Follow these steps:

1. Set up archive and purge routines.
2. Schedule monthly/weekly partition drops. Refer to [Section G.3.7.3, "Drop Scripts for Partitioned Tables."](#)
3. Schedule archive and purge routines.

G.3.2.2 Archive and Purge Process - Setting Up for Users with an Existing Process In Place

The setup scripts are one-time scripts that are required to create objects for the archive and purge process. The setup scripts will create the archived tables and store procedure required to execute during the routine archive and purge process.

If you are already using the Oracle Adaptive Access Manager Archive and Purge process, you should back up your existing archived tables (listed in [Section G.3.6, "Archive and Purge Details"](#)) on disk before setting up a new archive and purge process. With 10.1.4.5.bp2, the structure of the old tables has changed; the setup scripts will recreate these tables.

G.3.2.3 Archive and Purge Process - Setting Up for the Oracle Database

The `create_purge_proc.sql` script is required to set up the archive and purge routines for the Oracle Database. For more information on this script, refer to [Section G.3.7.1, "Scripts for the Oracle Database."](#)

G.3.2.3.1 Prerequisite

Important

You must ensure that the Oracle Adaptive Access Manager schema has the following privileges granted before the execution of the purging/archiving scripts and revoked after the execution of the purging/archiving scripts:

- `create procedure`
- `execute procedure`
- `create any procedure`
- `create any table`
- `create any index`

The purging/archiving scripts need `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 purge/archiving process is completed.

G.3.2.3.2 Instructions To set up the archive and purge process for the Oracle Database, follow these steps:

1. Create the script directory, `oaam_purge_script`.
2. Unzip the Oracle Adaptive Access Manager purge package Oracle scripts to the script directory.
3. Log in to the database using the `system` or `sys` account.
4. Grant privileges to the Oracle Adaptive Access Manager schema:

```
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. Connect to database using the Oracle Adaptive Access Manager schema.

```
For example, sqlplus <OAMADMIN>/<PASSWORD>
```

6. Run the `create_purge_proc.sql` script

```
SQL>@ create_purge_proc.sql
```

G.3.3 Performing Archive and Purge

The execution of the archive and purge scripts is described in this subsection. Before starting the archive and purge process, go through the following checklist to ensure that the requirements for archive and purge are met.

- Set up of the archive and purge scripts.
- Enough space is available on the database server to store the archived data, if archive is enabled for the purge.
- Archive and purge could be resource (like CPU) intensive. Oracle recommends running these during off peak load hours.

The required scripts to execute archive and purge routines for the Oracle Database are listed. For more information on these scripts, refer to [Section G.3.7.2, "Scripts to Execute Archive and Purge."](#)

Archive and purge periods are set based on the business requirement specified for retention periods.

By default, the archive and purge scripts/routines have the following two parameters set:

- `p_days1` =no of days for data retention
- `p_archived`= archived flag

To change these values per the business requirement, modify the following scripts:

- `exec_sp_purge_tracker_data.sql`
- `exec_sp_purge_txn_log.sql`
- `exec_sp_purge_workflow_data.sql`
- `exec_sp_purge_profile_data.sql`
- `exec_sp_purge_rule_log.sql`

G.3.3.1 Manual Execution

To execute the scripts to archive and purge, follow these steps:

1. Create the script directory, `oaam_purge_script`
2. Unzip the Oracle Adaptive Access Manager archive and purge package Oracle scripts to the script directory.
3. Log in to the database using the Oracle Adaptive Access Manager schema

For example,

```
sqlplus <OAMADMIN>/<PASSWORD>
```

4. Run the purging execution scripts:

```
SQL>@ exec_sp_purge_tracker_data.sql
SQL>@ exec_sp_purge_txn_log.sql
SQL>@ exec_sp_purge_workflow_data.sql
SQL>@ exec_sp_purge_profile_data.sql
SQL>@ exec_sp_purge_rule_log.sql
```

G.3.3.2 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.

G.3.4 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.

G.3.5 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.

G.3.6 Archive and Purge Details

This section contains information about the tables and their corresponding archived tables and details on the setup scripts.

Device fingerprint, autolearning transactional, transaction, and rule log tables and their corresponding tables are listed in the tables that follow.

G.3.6.1 Device Fingerprint Tables and Corresponding Archived Tables

Device Fingerprint Transaction 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

G.3.6.2 Autolearning Transactional Tables and Corresponding Archive 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

Autolearning Transactional Tables	Corresponding Archived Tables
V_FPRINTS	V_FPRINTS_PURGE
V_FP_MAP	V_FP_MAP_PURGE
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

G.3.6.3 Transaction Tables and Corresponding Archived 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

G.3.6.4 Rule Logs Tables and Corresponding Archived Tables

Rule 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

G.3.7 Scripts to Set Up Archive and Purge

Archive and purge setup scripts for the Oracle and SQL server databases are listed in the sections that follow.

G.3.7.1 Scripts for the Oracle Database

The archive and purge setup scripts for the Oracle Database are listed in this subsection.

G.3.7.1.1 create_purge_proc.sql The `create_purge_proc.sql` script creates the tables (Listed in [Section G.3.6, "Archive and Purge Details"](#)) and 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

G.3.7.2 Scripts to Execute Archive and Purge

The scripts to execute the archive and purge process are listed in the subsections following.

G.3.7.2.1 exec_sp_purge_tracker_data.sql This script calls stored procedures to archive and purge data from device fingerprinting tables. By running this script, the following tables will be archived and purged:

- VCRYPT_TRACKER_NODE
- VCRYPT_TRACKER_NODE_HISTORY
- VCRYPT_TRACKER_USERNODE_LOGS
- VT_USER_DEVICE_MAP

- VT_DYN_ACT_EXEC_LOG
- VT_SESSION_ACTION_MAP

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.

G.3.7.2.2 `exec_sp_purge_txn_log.sql` This script calls stored procedures to archive and purge data from in-session transaction tables. By running this script, the following tables will be archived and purged:

- VT_ENTITY_ONE
- VT_ENTITY_ONE_PROFILE
- VT_ENT_TRX_MAP
- VT_TRX_DATA
- VT_TRX_LOGS
- VT_USER_ENTITY1_MAP

G.3.7.2.3 `exec_sp_purge_workflow_data.sql` This script calls stored procedures to archive and purge data from the Workflow Autolearning tables. By running this script, the following tables will be archived and purged:

- VT_WF_DAYS
- VT_WF_HOURS
- VT_WF_MONTHS
- VT_WF_YEARS
- V_FPRINTS
- V_FP_MAP

G.3.7.2.4 `exec_sp_purge_profile_data.sql` This script calls stored procedures to archive and purge data from the Autolearning profile tables. By running this script, the following tables will be archived and purged:

- VT_BASE_IP_PROFILE
- VT_IP_PROFILE
- VT_DEVICE_PROFILE
- VT_COUNTRY_PROFILE
- VT_CITY_PROFILE
- VT_STATE_PROFILE
- VT_USER_PROFILE

G.3.7.2.5 `exec_sp_purge_rule_log.sql` This script calls stored procedures to archive and purge data from the Rules Engine logging tables. By running this script, the following tables will be archived and purged:

- VR_POLICYSET_LOGS
- VR_RULE_LOGS
- VR_MODEL_LOGS
- VR_POLICY_LOGS

G.3.7.3 Drop Scripts for Partitioned Tables

Two scripts to drop partitions are described in subsections that follow.

G.3.7.3.1 Drop_Monthly_Partition_tables.sql Use this script to drop partitions for tables with the monthly frequency. Run this script at the end of each month to drop partitions that are older than sixth months as per the Oracle Adaptive Access Manager application requirement. Eventually, these tables will have six partitions at any point.

G.3.7.3.2 Drop_Weekly_Partition_tables.sql Use this script to drop partitions for tables with the weekly frequency. Run this script at the end of every two weeks, starting from your database creation date, to drop partitions older than two weeks as per the Oracle Adaptive Access Manager application requirement.

G.4 Case Data Archive and Purge

This section presents the prerequisites and post-process procedures in archiving and purging case data in the Oracle Adaptive Access Manager database. A DBA or system administrator, who performs routine maintenance and the archiving and purging of case data in the Oracle Adaptive Access Manager database, should follow these instructions.

For a definition of purge, refer to [Section G.1, "Purge Process."](#)

For a definition of archive, refer to [Section G.2, "Archive Process."](#)

G.4.1 Archive and Purge Process for Case Data

The setup scripts are one-time scripts that are required to create objects for the archive and purge process for case data. The setup scripts will create the archived tables and store procedure required to execute during the routine archive and purge process for case data.

The procedures you will perform to archive and purge case data are:

1. Set up archive and purge case data routines.
2. Schedule monthly/weekly partition drops. Refer to [Section G.3.7.3, "Drop Scripts for Partitioned Tables."](#)
3. Schedule archive and purge routines.

G.4.1.1 Set Up the Archive and Purge Script

Set up instructions are provided in the following subsections.

Special Instructions

Case-related data purging is not intended for all the customers. The following instructions should only be used by the customers who have business requirement to purge old case-related data.

G.4.1.1.1 Prerequisite You must ensure that the Oracle Adaptive Access Manager schema has the following privileges granted before the execution of the purging/archiving script:

- Create procedure
- Execute procedure
- Create any procedure
- Create any table
- Create any index

G.4.1.1.2 Set Up Archive and Purge Script The `create_case_purge_proc.sql` script is required to set up the archive and purge routines for the Oracle database. For more information on this script, refer to [Section G.4.1.5.2, "create_case_purge_proc.sql - Setup Script for Archive and Purge."](#)

To set up the archive and purge process, follow these steps:

1. Create the script directory, `oaam_purge_script`.
2. Unzip the Oracle Adaptive Access Manager purge package, `case_purge_scripts`, to the script directory.
3. Log in to the database using the `system` or `sys` account.
4. Grant privileges to the Oracle Adaptive Access Manager schema:

```
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. Connect to database using the Oracle Adaptive Access Manager schema.

```
For example, sqlplus <OAAMADMIN>/<PASSWORD>
```

6. Run the `create_case_purge_proc.sql` script

```
SQL>@ create_case_purge_proc.sql
```

G.4.1.2 Execute Archive and Purge Script

The execution of the archive and purge script is described in this subsection. Prior to starting the archive and purge process, go through the following checklist to ensure that the requirements for archive and purge are met.

- Setup of the archive and purge script. Refer to [Section G.4.1.1.2, "Set Up Archive and Purge Script."](#)
- Enough space is available on the database server to store the archived data, if archive is enabled for the purge.
- Archive and purge could be resource (like CPU) intensive. Oracle recommends running these during off peak load hours.

For information on the required script to execute archive and purge routines for case data, refer to [Section G.4.1.5.3, "exec_purge_case_data.sql - Execution Script for Archive and purge execution script."](#)

Archive and purge periods are set based on the business requirement specified for retention periods.

By default, the archive and purge script has the following two parameters set:

- `p_days1` =no of days for data retention
- `p_archived`= archived flag

To change these values per the business requirement, modify the `exec_sp_purge_case_data.sql`.

G.4.1.2.1 Manual Execution To execute the script to archive and purge, follow these steps:

1. Create the script directory, `oaam_purge_script`.
2. Unzip the Oracle Adaptive Access Manager purge package, `case_purge_scripts`, to the script directory.
3. Log in to the database using the Oracle Adaptive Access Manager schema

For example,

```
sqlplus <OAAMADMIN>/<PASSWORD>
```

4. Run the `exec_sp_purge_case_data.sql` script

```
SQL>@ exec_sp_purge_case_data.sql
```

G.4.1.2.2 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.

G.4.1.3 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, you can also query the transactional log and its related purged tables to validate that the data was archived and purged.

G.4.1.4 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.

G.4.1.5 Case Data Archive and Purge Details

This section contains information about the tables and their corresponding archived tables and details on the setup script.

G.4.1.5.1 Case-Related Tables and Their Corresponding Archived Tables For your reference case-related tables and their corresponding archived tables are listed:

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

G.4.1.5.2 create_case_purge_proc.sql - Setup Script for Archive and Purge The create_case_purge_proc.sql script creates the tables listed in [Section G.4.1.5.1, "Case-Related Tables and Their Corresponding Archived Tables"](#) and 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

G.4.1.5.3 exec_purge_case_data.sql - Execution Script for Archive and purge execution script

The exec_purge_case_data.sql script calls the stored procedures to archive and purge data from device fingerprinting tables. By running this script, the following tables will be archived and purged:

- V_CASE
- V_CASE_HIST
- V_ACTION_LOG_SESS_MAP
- V_ACTION_LOG_SESS
- V_CASE_MAP
- V_CASE_MAP_HIST

G.5 Monitor Data Archive and Purge

This section presents the prerequisites and post-process procedures in archiving and purging monitor data in the Oracle Adaptive Access Manager database. A DBA or system administrator, who performs routine maintenance and the archiving and purging of data in the Oracle Adaptive Access Manager database, should follow these instructions.

For a definition of purge, refer to [Section G.1, "Purge Process."](#)

For a definition of archive, refer to [Section G.2, "Archive Process."](#)

G.5.1 Archive and Purge Process for Monitor Data

The setup scripts are one-time scripts that are required to create objects for the archive and purge process for monitor data. The setup scripts will create the archived tables

and store procedure required to execute during the routine archive and purge process for monitor data.

The procedures to perform to archive and purge monitor data are:

1. Set up archive and purge monitor data routines.
2. Schedule monthly/weekly partition drops. Refer to [Section G.3.7.3, "Drop Scripts for Partitioned Tables."](#)
3. Schedule archive and purge routines.

G.5.1.1 Set Up the Archive and Purge Script

Set up instructions are provided in the following subsections.

G.5.1.1.1 Special Instructions - Dropping the Monitor Data

Customers who are using the Oracle table partitioning option and have no reporting database should run the `drop_monitor_partition.sql` script before setting up purging routine for monitor data.

To do so, follow these steps:

1. Create the script directory, `oaam_purge_script`.
2. Unzip the Oracle Adaptive Access Manager purge package, `monitor_purge`, to the script directory.
3. Log in to the database using the `system` or `sys` account.
4. Grant privileges to the Oracle Adaptive Access Manager schema:

```
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. Connect to database using the Oracle Adaptive Access Manager schema.

```
For example, sqlplus <OAMADMIN>/<PASSWORD>
```

6. Run the purging execution script

```
SQL>@ drop_monitor_partition.sql
```

G.5.1.1.2 Prerequisite - Privileges Granted to Schema You must ensure that the Oracle Adaptive Access Manager schema has the following privileges granted before the execution of the purging/archiving script:

- Create procedure
- Execute procedure
- Create any procedure
- Create any table
- Create any index

G.5.1.1.3 Set Up Archive and Purge Instructions The `create_v_monitor_purge_proc.sql` script is required to set up the archive and purge routines for the Oracle database. For

more information on this script, refer to [Section G.5.1.5.2, "create_v_monitor_purge_proc.sql - Setup Script for Archive and Purge."](#)

To set up the archive and purge process, follow these steps:

1. Create the script directory, `oaam_purge_script`.
2. Unzip the Oracle Adaptive Access Manager purge package, `monitor_purge`, to the script directory.
3. Log in to the database using the `system` or `sys` account.
4. Grant privileges to the Oracle Adaptive Access Manager schema:

```
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. Connect to database using the Oracle Adaptive Access Manager schema.

For example, `sqlplus <OAMADMIN>/<PASSWORD>`

6. Run the create script

```
SQL>@ create_v_monitor_purge_proc.sql
```

G.5.1.2 Execute Archive and Purge Script

The execution of the archive and purge script is described in this subsection. Prior to starting the archive and purge process, go through the following checklist to ensure that the requirements for archive and purge are met.

- Setup of the archive and purge script. Refer to [Section G.5.1.1.3, "Set Up Archive and Purge Instructions."](#)
- Enough space is available on the database server to store the archived data, if archive is enabled for the purge.
- Archive and purge could be resource (like CPU) intensive. Oracle recommends running these during off peak load hours.

The required script to execute archive and purge routines for the monitor data is the `exec_v_monitor_purge_proc.sql` script. For a description, refer to [Section G.5.1.5.3, "exec_v_monitor_purge_proc.sql - Execution Script for Archive and purge execution script."](#)

Archive and purge periods are set based on the business requirement specified for retention periods.

By default, the archive and purge script has the following two parameters set:

- `p_days1` =no of days for data retention
- `p_archived`= archived flag

To change these values per the business requirement, modify the `exec_v_monitor_purge_proc.sql`.

G.5.1.2.1 Manual Execution To execute the script to archive and purge, follow these steps:

1. Create the script directory, `oaam_purge_script`.

2. Unzip the Oracle Adaptive Access Manager purge package, `monitor_purge`, to the script directory.

3. Log in to the database using the Oracle Adaptive Access Manager schema

For example,

```
sqlplus <OAADMIN>/<PASSWORD>
```

4. Run the `exec_v_monitor_purge_proc.sql` script

```
SQL>@ exec_v_monitor_purge_proc.sql
```

G.5.1.2.2 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.

G.5.1.3 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, you can also query the transactional log and its related purged tables to validate that the data was archived and purged.

G.5.1.4 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.

G.5.1.5 Monitor Data Archive and Purge Details

This section contains information about the tables and their corresponding archived tables and details on the setup script.

G.5.1.5.1 Monitor Data-Related Table and the Corresponding Archived Table For your reference the monitor data-related table and its corresponding archived table is listed.

Transaction Table	Corresponding Archived Table
V_MONITOR_DATA	V_MONITOR_DATA_PURGE

G.5.1.5.2 create_v_monitor_purge_proc.sql - Setup Script for Archive and Purge The `create_v_monitor_purge_proc.sql` script creates the `V_MONITOR_DATA_PURGE` table listed in [Section G.5.1.5.1, "Monitor Data-Related Table and the Corresponding Archived Table"](#) and the following stored procedure, `SP_V_MON_DATA_PURGE_PROC`, to archive and purge data from the transaction table.

G.5.1.5.3 exec_v_monitor_purge_proc.sql - Execution Script for Archive and purge execution script The `exec_v_monitor_purge_proc.sql` script calls the stored procedures to archive and purge data from device fingerprinting tables. By running this script, the `V_MONITOR_DATA` table will be archived and purged.

Configuring Logging Output

Logging is the mechanism by which components write messages to a file.

Oracle Adaptive Access Manager 11g components use the package `java.util.logging` as part of its logging infrastructure. This package is available in all Java environments.

The logging configuration can be initialized using a logging configuration file that will be read at startup.

The default logging configuration file, `logging.properties`, is located in the Home directory. It configures the Oracle Adaptive Access Manager Framework loggers to print messages. You can edit the file to specify the level of detail in the log messages. For example, you can specify whether log messages are sent to the console, to a file or to both. In addition, you can specify logging at the level of individual areas for which a logger is defined.

H.1 Handlers

The Java logging utility, `java.util.logging`, uses handler classes to output log messages.

[Appendix H-1](#) shows the handlers used by Oracle Adaptive Access Manager

Table H-1 Handler Classes

Handler Class	Function
<code>FileHandler</code>	A handler that writes formatted log records either to a single file, or to a set of rotating log files.
<code>ConsoleHandler</code>	A simple handler for writing formatted records to <code>System.err</code>

H.1.1 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.

H.1.2 Configuring Both Console Logging and File Logging

You can set the logging utility 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
```

H.2 Oracle Adaptive Access Manager Loggers

A Logger is used to log messages for a specific component. Oracle Adaptive Access Manager Loggers are described in [Table H-2](#).

Table H-2 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

H.3 Logging Levels

Each log message has an associated log Level. The Level gives a rough guide to the importance and urgency of a log message. Each log level has an integer value, with higher values indicating higher priorities.

Levels of logging are ALL, TRACE, FINEST, FINER, FINE, CONFIG, INFO, WARNING, SEVERE, and OFF.

Details about Java Logging:

1. Any logging at INFO and above provides complete details
2. SEVERE is used to diagnose if there is improper functioning of the system.
3. Any logging message below INFO should have its logging enabled to check for performance reasons (`isDebugEnabled()` / `isLevelEnabled()`).

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
```

H.4 Other Properties

To redirect oracle.oaam and child 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
```

Rule and Fingerprint Logging

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 11g, 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.

I.1 Detailed Rule Logging

Detailed rule logging captures the time taken at each rule level.

I.1.1 Enabling Detailed Rule Logging

The steps to enable detailed rule logging are:

1. In the Navigation tree, double-click **Properties** under **Environment**.
2. Enter **vcrypt.tracker.rules.trace.policySet** in the **Name** field and click **Search**.
3. In the Results table, select **vcrypt.tracker.rules.trace.policySet**.
4. In the Details **vcrypt.tracker.rules.trace.policySet** section, enter **true** in the **Value** field.
5. Click **Save**.
A confirmation dialog is displayed.
6. Click **OK** to dismiss the dialog.
7. Specify checkpoint to log rules.

I.1.2 Specifying When to Log

The steps to specify the checkpoint in which to log are:

1. In the Navigation tree, double-click **Properties** under **Environment**.

2. Click the **New Property** button or the **Create new property** icon.
3. Enter `vcrypt.tracker.rules.trace.policySet.<checkpoint string value>` in the **Name** field.
4. Enter `true` in the **Value** field and click **Create**.

I.1.3 Configuring Detailed Logging Threshold Time

For detailed rule logging, you can configure a threshold time value, "x," so that logging is performed only if the time taken for the rule is greater than the threshold value.

To modify the threshold time after which the rule logging should begin, follow these steps:

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 "x" in milliseconds specified, Oracle Adaptive Access Manager starts the detailed rule logging.

I.1.4 Rule Logging Flow

In the next sections, the Post-Authentication checkpoint is used to illustrate rule logging.

In detailed rule logging, the flow is as follows:

1. The Rules Engine checks for a `vcrypt.tracker.rules.trace.policySet.<checkpoint string value>` configuration.
For example, `vcrypt.tracker.rules.trace.policySet.postauth`.
2. If there is no configuration for `vcrypt.tracker.rules.trace.policySet.postauth`, the Rules Engine checks the value of `vcrypt.tracker.rules.trace.policySet`.
By default, the value for `vcrypt.tracker.rules.trace.policySet` is set to "true".

The values of the two properties determine whether rule logging is enabled for a given checkpoint.

Refer to [Section I.1.5, "Value Combinations"](#) for details on value combinations that specify rule logging.

I.1.5 Value Combinations

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 during a specified checkpoint.

The Post-Authentication checkpoint is used in this example.

value of <code>vcrypt.tracker.rules.trace.policySet.postauth</code>	value of <code>vcrypt.tracker.rules.trace.policySet</code>	Will Rule logging be enabled for the postauth checkpoint?
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

I.1.6 Logging Non-Triggered Rules

The properties to control the logging of rules that did not trigger are:

```
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 non-triggered rules exceeds the value of `vcrypt.tracker.rules.trace.notTriggered.logMillis`, only then will the Rules Engine log the non-triggered Rules.

I.1.6.1 Examples

The following table shows the property values that control what non-triggered rules are logged.

<code>vcrypt.tracker.rules.trace.notTriggered</code>	<code>vcrypt.tracker.rules.trace.notTriggered.logMillis</code>	Result
true	n	Logs the non-triggered Rules that took more than "n". If "n" is set to a negative value, all Rules are logged

<code>vcrypt.tracker.rules.trace.notTriggered</code>	<code>vcrypt.tracker.rules.trace.notTriggered.logMillis</code>	Result
false	n	None of the non-triggered Rules will be logged

I.2 Enabling Fingerprint Rule Logging

To enable or disable fingerprint rule logging, modify the following property

```
vcrypt.tracker.rulelog.fingerprint.enabled=true
```

I.3 Specifying Properties in Running Both Fingerprint and Detailed Logging

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=
```

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?"

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.

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

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.

Checkpoint

When a policy is called to run its rules. 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 we use 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 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

Device

A computer, PDA, cell phone, kiosk, etc used by a user

Device Fingerprinting

A mechanism to recognize the device a customer typically uses to log in – whether it is a desktop computer, laptop computer, PDA, cell phone, kiosk, or other web enabled device. The fingerprinting process produces a fingerprint that is unique to the user and designed to protect against the "replay attacks" and the "cookie based registration bypass" process.

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're closed. If a case has any status besides closed, the disposition is left blank.

Device Registration

Device registration is a feature that allows a user to flag the device (computer, mobile, PDA, and others) 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.

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.

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, we 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

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)

OOAM 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.

Multitenant

Multitenancy refers to a principle in software architecture where a single instance of the software runs on a server, serving multiple client organizations (tenants).

With a multitenant architecture, a software application is designed to virtually partition its data and configuration so that each client organization works with a customized virtual application instance.

The distinction between the customers is achieved during application design, so that customers do not share or see each other's data.

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.

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.

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 usernames, passwords and credit card details, by masquerading as a trustworthy entity. Often a phishing exercise starts with an email aimed to lure in gullible users.

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.

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 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

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.

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

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.

Numerics

- 11g architecture, 1-5
- 11g vs. 10g
 - feature comparison chart, 0-xxxii
 - key conceptual and terminology changes, 0-xxxiv

A

- abbreviation file, adding to, 6-34, F-5
- access management integration, 1-5
- Action and Alert Overrides, 12-6
- Action and Score Overrides, 11-2
- action instances
 - Action Priority, 15-10
 - creating, 15-8
 - edit, 15-13, 15-14
 - execution types, 15-8
 - search page, 15-7
 - Time to Live, 15-10
- action override
 - adding or editing, 11-4
 - creating, 11-4
- action templates, 15-1
 - creating, 15-5
 - deleting, 15-13
 - details, 15-5
 - editing, 15-12
 - exporting, 15-12
 - importing, 15-12
 - search page, 15-4
- actions, 9-4
- Actions group, 10-1, 10-17
- activate
 - challenge questions, 6-20
 - entities, 16-9, 16-11
 - patterns, 14-19
 - transaction definitions, 17-10
- add
 - answer validation, 6-21
 - members to a new or an existing group, 10-9
 - OTP device, 8-6
- AddItemToListAction, 15-15
- Address entity, 16-1
- Aggregate scoring engine, 12-3
- alerts, 9-5
- Alerts group, 10-1
- AlertsBreakdown report, C-2
- Always On - User, B-1
- anonymizer data, 23-18
- anonymizer data, loading, 23-13
- Answer Logic
 - configuring, 6-29
- Answer Logic algorithms
 - common abbreviations, 6-31
 - common misspellings, 6-31
 - common nicknames, 6-31
 - common typos, 6-32
 - date format, 6-31
 - keyboard fat fingering, 6-32
 - phonetics, 6-31
- answer logic algorithms
 - fat fingering algorithm, F-5
 - phonetics, F-4
- Answer Logic level, 6-32
 - abbreviation, 6-32
 - fat fingering, 6-33
 - multiple word answers, 6-33
 - phonetics, 6-33
- answer registration validations, 6-20
- answer validation
 - adding, 6-21
- Application ID, 0-xxxiv, 24-3
- archive and purge procedures, G-1
- ASN, 10-1
- ASN group, 10-1, 10-11
- asynchronous actions, 15-8
- attributes, 14-3
- Audit Information
 - Customer Care Events, 21-2
 - Group/List Management Events, 21-4
 - KBA Questions Events, 21-3
 - Policy Management Events, 21-2
 - sent to Audit System, 21-2
- Authentication Status group, 10-1, 10-17
- authentication-related entities, importing, 2-8
- autolearning, 14-1, Glossary-2
 - APIs for triggering pattern data processing, A-2
 - data/profiling data, 14-22
 - enabling, 2-9, 14-8
 - in native integration, 14-10
 - pattern creations, best practices, 14-14

- pattern data processing (On-Line and Scheduled), A-1
- Autonomous System Numbers, 10-1
- Average scoring engine, 12-3
- AveragesSummary report, C-3

B

- basic environment setup
 - autolearning enabling, 2-9
 - CLI, 2-2
 - configurable actions
 - enabling, 2-9
 - encryption and database credentials, 2-2
- bharosa.trackeradmin.show.transaction.detail, 5-1
- bharosa.uio.default.challenge.type.enum.ChallengeQuestion.available, 8-7
- bharosa.uio.default.register.userinfo.enabled, 8-4
- bharosa.uio.default.use.authentipad.checkpoint, 8-6
- bharosa.uio.default.userinfo.inputs.enum, 8-4
- bharosa.uio.default.userpreferences.userinfo.enabled, 8-4
- BI Publisher reports, C-1
 - configuring, 19-1
- bucket, 14-3
 - creation and population, 14-2
 - population, 14-8
- business analysts, 3-2
 - security analyst, 1-4
- By Digest, 16-7
- By Key, 16-7

C

- Cache Policy, 10-6
- case
 - actions, 4-10
 - activity log, 4-11
 - activity, viewing, 4-11
 - best practices and recommendations, 4-35
 - close multiple at once, 4-17
 - Closed status, 4-27
 - closing, 4-28
 - create like, 4-16
 - creating, 4-14
 - CSR, 4-1, 4-2
 - definition, 4-2
 - description keyword, searching by, 4-9
 - details, viewing, 4-10
 - escalated, 4-2
 - escalated case logs, 4-12
 - Escalated status, 4-27
 - escalating, 4-29
 - expiration date, 4-4
 - expiry behavior, 4-29
 - extending expiration, 4-29
 - history, viewing, 4-11
 - log, searching, 4-12
 - management, 1-2

- New status, 4-27
- notes, adding, 4-25
- open and closed, searching, 4-8
- Pending status, 4-27
- reopening closed cases, 4-28
- severity level, 4-4
- severity level, changing, 4-26
- status, 4-4
- status, changing, 4-26
- user details, viewing, 4-10
- Case Details page, 4-9
- CaseCreationAction, 15-14
- Cases search page, 4-6
- cases, bulk editing, 4-17
- challenge questions
 - activating, 6-20
 - Answer Logic, 6-5
 - categories, 6-3
 - create like, 6-17
 - creating, 6-36
 - creating new, 6-16
 - deactivating, 6-20
 - deleting, 6-19
 - details and statistics, 6-16
 - disabling, 6-19
 - editing, 6-18
 - enabling, 7-1
 - exporting, 6-18
 - Global Registration Validation (Global), 6-6
 - Global-Local validation, 6-7
 - importing, 2-6, 6-18
 - increment to next question, 4-24
 - increment user to the next challenge question, 6-8
 - managing, 6-13
 - Question Registration Validation (Local), 6-6
 - question set, 6-3
 - registration, 6-2
 - registration logic, 6-3
 - resets, 4-22
 - resetting, 4-23, 6-7
 - searching for, 6-14
 - validate challenge question answers, 6-6
- challenge questions, importing, 6-9
- challenge response
 - configuration, 6-2
 - process, 6-2
- challenge setup
 - answer logic, 6-10
 - registration logic, 6-10
- ChallengeStatistics report, C-2
- checkpoints, 0-xxxiv, 9-3
 - example, 9-4
- Cities group, 10-2, 10-11, 10-12
- City Confidence Factor, 9-31
- CLI
 - basic environment setup, 2-2
 - export options, 23-8
 - import of files, 23-7
 - import options, 23-10
 - importing multiple types of entities in one

- transaction, 23-10
- obtaining usage information for import or export, 23-5
- options, 23-5
- parameters, 23-6
- setting up the environment, 23-1
- transaction handling, 23-11
- verview, 23-1
- com.bharosa.vcrypt.tracker.dynamicactions.intf.Dyna micAction java interface, 15-11
- Command-Line Interface (CLI), 23-1
- conditions, 9-3
 - adding conditions to a rule, 9-34
 - deleting, 9-38
 - deleting from a rule, 9-38
 - details of a rule, 9-36
 - editing, 9-37
 - exporting, 9-37
 - importing, 9-34
 - order in a rule, 9-37
 - searching for, 9-33
- conditions library, importing, 2-8
- config_secret_key.file, 2-3
- configurable action instances, 15-13
- configurable actions, 1-3, 15-1
 - adding to runtime, 15-8, 15-13
 - creating, 15-3
 - deploying, 15-2
 - enabling, 2-9
 - out-of-the-box, 15-14
 - standard, 15-14
 - templates, importing, 2-8
- configurable actions, defining, 15-5
- configurable actions, viewing, 15-8, 15-13
- configure
 - Answer Logic, 6-29
 - OTP challenge type, 8-5
 - OTP delivery, 8-6
 - OTP presentation, 8-6
 - registration logic, 6-27
- connection speed
 - group, 10-2
- Connection Speed group, 10-17
- connection speed mapping, 23-17
- Connection Type group, 10-17
- connection types
 - roup, 10-2
- connection types mapping, 23-16
- copying
 - policy to another checkpoint, 9-24
 - rule to policy, 9-19, 9-23
- Countries group, 10-2, 10-11
- Country Confidence Factor, 9-31
- Country group, 10-12
- CountryAggregates report, C-2
- create
 - action templates, 15-5
 - challenge questions, 6-36
 - entities, 16-4
 - patterns, 14-14
 - policies, 9-7, 9-11
 - transaction definitions, 17-6
- create like
 - challenge questions, 6-17
- create new
 - challenge questions, 6-16
- Credential Store Framework, 2-2
- credit card entity, 16-1
- CSR and CSR Manager role permissions, 4-5
- CSR Manager, 4-3
- custom action instances
 - creating, 15-11
- customer
 - logins, filter by authentication status or alert level, 4-14
 - logins, search by device or date range, 4-13
 - logins, viewing, 4-13
 - profile, resetting, 4-22
 - resets, 4-4, 4-18
 - service representative (CSR), 4-2
 - service representatives (CSR), 1-4, 3-2
 - session history, viewing, 4-13
 - sessions, searching, 4-13
 - sessions, viewing, 4-12

D

- dashboard, 1-2, 18-1
 - Performance panel, 18-2
 - Summary panel, 18-4
 - viewing performance, 18-2
- dashboards, 18-5
 - viewing browser and OS data by device, 18-8
 - viewing data type by performance, 18-8
 - viewing list of rule or alerts by security, 18-7
 - viewing list of scoring breakdowns, 18-7
- data elements, 16-1
- Data Identification Scheme, 16-7
- database credentials
 - setup, 2-2
- database credentials in the Credential Store Framework, 2-6
- deactivate
 - challenge questions, 6-20
 - entities, 16-11
 - patterns, 14-19
 - transaction
 - definitions, 17-12
- define
 - groups, 10-8
 - OTP email challenge, 8-6
- delete
 - action templates, 15-13
 - challenge questions, 6-19
 - conditions, 9-38
 - entities, 16-12
 - groups, 10-22
 - patterns, 14-22
 - policies, 9-23
 - rules, 9-32

- transaction definitions, 17-13
- DESede_config_key_alias, 2-5
- DESede_db_key_alias, 2-5
- Device
 - Browser header substring, B-1, B-7
 - Device first-time for user, B-1
 - Device firsttime for user, B-7
 - Device in list, B-1
 - Excessive Use, B-8
 - Excessive use, B-1
 - fingerprinting data archive and purge
 - criteria, G-1
 - In Group, B-8
 - Is registered, B-1, B-9
 - Login Count, B-1
 - Timed not status, B-1, B-10
 - Used count for User, B-11
 - Used count for user, B-1
 - User count, B-10
 - User status count, B-1
 - Velocity from last login, B-1, B-12
- Device ID
 - Cookie state, B-1
 - Cookies match, B-1
 - Header data match, B-1
 - Header data match percentage, B-1
 - Header data present, B-1
 - HTTP header data browser match, B-2
 - HTTP header data browser upgrade, B-2
 - HTTP header data operating system match, B-2
 - HTTP header data operating system
 - upgrade, B-2
 - Is Cookie disabled, B-1
 - Is Cookie empty, B-1
 - Is Cookie from same device, B-1
 - Is Cookie Old, B-1
 - Is Cookie Valid, B-1
 - known header data match percentage, B-2
 - User ASN first time, B-2
 - User Carrier first time, B-2
 - User City first time, B-2
 - User Country first time, B-2
 - User IP first time, B-2
 - User ISP first time, B-2
 - User State first time, B-2
 - User used this finger print, B-2
- Device Risk Gradient, 9-31
- DeviceIdScoring report, C-1
- Devices group, 10-2, 10-13
- devices, unregistering, 4-20
- disable
 - challenge questions, 6-19
 - logic for KBA, 6-8
- discovery process, E-1
- display elements, 16-2
- Dynamic Monitoring System (DMS), 21-1
- dynamicactions.enabled, 2-9

E

- edit
 - action templates, 15-12
 - challenge questions, 6-18
 - conditions, 9-37
 - entities, 16-10
 - patterns, 14-14, 14-19
 - policies, 9-15
 - policy set, 11-6
 - transaction definitions, 17-11
- employee entity, 17-1
- enable
 - challenge questions, 7-1
 - OTP challenges, 8-7
- encoded secret key, generating, 2-5
- encodeKey command, 2-2
- encryption
 - key, 2-2
 - setup, 2-2
- entities, 16-1, 17-1
 - activating, 16-9, 16-11
 - creating, 16-4
 - creation, best practices, 16-12
 - data elements, adding, 16-5
 - deactivating, 16-11
 - deleting, 16-12
 - details, viewing, 16-9
 - display scheme, specifying data for, 16-8
 - editing, 16-10
 - exporting, 16-10
 - ID Scheme, selecting, 16-6
 - importing, 16-11
 - reordering the rows in the ID Scheme and Display
 - tabs, 16-12
 - search page, 16-2
- Entity
 - Entity is a member of the bucket N times in a given
 - time period, B-2
 - Entity is member of bucket N times in a given time
 - period, B-17
 - Entity is member of pattern bucket for first time in
 - certain time period, B-2
 - Entity is Member of Pattern Bucket for the first
 - time in Certain Time Period, B-13
 - Entity is member of pattern bucket less than some
 - percent with all entities in picture, B-2, B-15
 - Entity is member of pattern less than some percent
 - times, B-2, B-14
 - Entity is member of pattern N times, B-2, B-16
- evaluation priority, 14-21
- Excluded User Group, 9-31
- expiration date for cases, 4-4
- expiration, cases, 4-29
- expiry behavior for cases
 - disabling, 4-29, D-2
 - setting, 4-29, D-2
- export
 - action templates, 15-12
 - challenge questions, 6-18
 - conditions, 9-37

- entities, 16-10
- groups, 10-21
- patterns, 14-22
- policies, 9-25
- transaction definitions, 17-11

Ext ID, 16-2

F

Fraud Investigation Manager, 4-3
Fraud Investigator, 4-3

G

genEncodedKey, 2-2
Generic Integers group, 10-11
Generic Longs group, 10-2, 10-11
Generic Strings group, 10-2, 10-11
Generics group, 10-2
globalization support, F-1
group linking, 9-5, 9-12
group types, 10-1
groups, 9-4, 10-1

- Actions, 10-1, 10-17
- add members from cities, states, and countries by filtering an existing list (no creation option), 10-9
- adding alerts, 10-10
- adding alerts to a group, 10-15
- adding members, 10-9
- Alerts, 10-1
- ASN, 10-1, 10-11
- Authentication Status, 10-1, 10-17
- characteristics, 10-7
- Cities, 10-2, 10-11, 10-12
- Connection Speed, 10-2, 10-17
- Connection Type, 10-2, 10-17
- Countries, 10-2, 10-11, 10-12
- create a new member to add to the group, 10-9
- creating a new element/member to add to the group (no search and filter options), 10-11
- defining, 10-8
- deleting, 10-22
- details page, 10-6
- Devices, 10-2, 10-13
- editing, 10-20
- exporting, 10-21
- exporting and importing, 10-21
- filtering an existing list to select an element to add to the group (no creation of a new element), 10-11
- Generic Integers, 10-11
- Generic Longs, 10-2, 10-11
- Generic Strings, 10-2, 10-11
- Generics, 10-2
- importing, 10-22
- IP, 10-2, 10-13
- IP Carriers, 10-2, 10-11
- IP Range, 10-13
- IP Ranges, 10-2

ISP, 10-2, 10-13

- member, editing, 10-20
- removing a user from a User Group, 10-21
- removing members of, 10-21

Routing Type, 10-2, 10-17

search and add existing elements only (no creation), 10-10

search for existing elements or create new elements, 10-10

search page, 10-4

searching for, 10-5

searching for and adding existing elements, 10-17

searching for and adding existing elements or creating and adding a new element, 10-13

Second-Level Domains, 10-2, 10-11

States, 10-2, 10-11, 10-12

Top-Level Domains, 10-3, 10-11

transaction

- status, 10-3, 10-17

updating directly, 10-23

usage, 10-3

User ID, 10-3, 10-13

Username, 10-2, 10-13

viewing details about, 10-6

I

ID scheme, 16-2

image and phrase, resetting, 4-20

image, resetting, 4-18

import

- action templates, 15-12
- authentication-related entities, 2-8
- challenge questions, 2-6, 6-9, 6-18
- conditions, 9-34
- conditions library, 2-8
- configurable actions
 - templates, 2-8
- entities, 16-11
- groups, 10-22
- IP
 - location data, 2-8
 - patterns, 14-21
 - policies, 2-7, 9-6, 9-25
 - transaction definitions, 17-12
- increment step size, 14-5
- incrementing to next challenge question, 4-24
- in-session transaction data archive and purge criteria, G-2

integration

- access management, 1-5
 - native, 1-4
 - Oracle Adaptive Access Manager, 1-4
 - reverse proxy, 1-5
 - SAML, 1-5
 - SOAP/Web services, 1-4
 - static linked (In Proc), 1-4
- internal identifier, 16-2

IP, 23-12

- carriers group, 10-2, 10-11

- group, 10-2, 10-13
- Loader properties, 23-13
- location data, importing, 2-8, 23-12
- Location Loader Properties, 23-12
- range group, 10-13
- ranges group, 10-2
- ISP group, 10-2, 10-13

K

- KBA, 1-3, 6-1
 - disabling logic for, 6-8
 - failure counter
 - setting up, 6-35
 - failure counters, 6-7
 - Locked status, 6-9
 - phone challenge, 4-24, 6-8
 - resets
 - reset
 - KBA, 6-7
 - security solution guidelines, 6-38
 - unlock a user, 6-8
- KBA vs. OTP, 8-2
- KeyStore command, 2-4

L

- loading MaxMind IP data, setting up for, 23-13
- Location
 - ASN in group, B-2, B-20
 - City in group, B-25
 - Domain in group, B-2
 - In carrier group, B-2, B-23
 - In City group, B-2
 - In Country group, B-3, B-21
 - IP Conn Speed in group, B-2
 - IP Conn Type in group, B-2
 - IP connection type, B-2
 - IP Connection type in group, B-22
 - IP Excessive use, B-3
 - IP in group, B-3
 - IP in Range group, B-20
 - IP in range group, B-3
 - IP is AOL, B-3
 - IP line speed type, B-3, B-22
 - IP Max logins, B-3
 - IP Max Users, B-3
 - IP Maximum Users, B-24
 - IP Multiple Devices, B-3
 - IP routing type, B-3
 - IP Routing Type in group, B-3, B-23
 - IP type, B-3
 - Is IP from AOL, B-25
 - ISP in group, B-3
 - State in group, B-3
 - Timed not status, B-3
 - Top Level Domain in group, B-3
 - User status count, B-3
- location
 - data, loading, 23-13

- loading tables, 23-18
- Locked status, 4-3
 - KBA, 6-9
 - OTP, 8-2
- logging, I-1
 - output, H-1
- LoginSummary report, C-3

M

- Maximum scoring engine, 12-3
- member types, 14-3
- member types and attributes, 14-3
- Microsoft SQL Server database, setting up, 23-12
- Minimum scoring engine, 12-3
- models
 - editing, 9-15
- monitor and audit of events, 21-1
- Monitoring Information
 - APIs Execution Information, 21-2
 - Login Information, 21-1
 - Rules Engine Execution Information, 21-1
- multi-bucket patterns, 14-4, Glossary-4
- MultipleDevices report, C-3
- MultipleFailures report, C-1
- MultipleUsers report, C-1, C-2
- multitenancy, 24-1

N

- native integration, 1-4
- Navigation tree
 - menu and toolbar, 3-6
- navigation tree, 3-5
- nested policies, 9-5
- new features, 11g, 0-xxxi
- notes, adding to cases, 4-25

O

- OAAM Admin, 0-xxxiv, 3-1
 - access level, 3-1
 - console and controls, 3-3
 - details pages, 3-16
 - management areas, 3-11
 - search pages, 3-13
 - sign in, 3-2
- OAAM Server, 0-xxxiv
- oaam_db_key, 2-6
- Online Help, 3-17
- Oracle Adaptive Access Manager Online Help, 3-17
- Oracle Adaptive Access Manager URL, 3-3
- Oracle Enterprise Manager Fusion Middleware Control, 25-14
- Oracle Fusion Middleware Control, 20-1
- Organization ID, 0-xxxiv, 4-15, 24-3
- OTP
 - case details, 8-9
 - case management, 8-8
 - challenge, 8-2
 - Challenge types, 8-4

- challenge types, configuring, 8-5
- challenges, enabling, 8-7
- contact input elements, 8-4
- delivery configuration, 8-6
- device used for challenges, changing, 8-7
- device, adding, 8-6
- email challenge, defining, 8-6
- email registration, 8-5
- failure counter, setting up, 8-8
- Failure Counters, 8-2
- Locked status, 8-2
- mobile device registration, 8-4
- new registration, 8-3
- performance data, viewing, 8-9
- preference setting, 8-4
- presentation, configuring, 8-6
- profile registration, 8-4
- profile, resetting, 8-3, 8-8
- Registration page, 8-4
- resetting, 8-3
- setting up, 8-3
- unlocking, 4-21
- unlocking customer, 8-3
- user login example, 8-3
- user, unlocking, 8-8
- OTP profile, resetting, 4-20

P

- pattern attributes operators
 - Equals, 14-33
 - For Each, 14-33
 - Greater Than, 14-33
 - Greater Than Equal To, 14-33
 - In, 14-34
 - Less Than, 14-33
 - Less Than Equal To, 14-33
 - Like, 14-34
 - Not Equal, 14-34
 - Not In, 14-34
 - Not Like, 14-34
 - Range, 14-34
- pattern rules evaluations, 14-6
- patterns, 14-1
 - activating, 14-19
 - adding attributes, 14-17
 - adding or changing member type, 14-20
 - changing status of, 14-20
 - creating, 14-14
 - creation method, 14-13
 - data processing, A-1
 - deactivate, 14-19
 - deactivating and activating, 14-19
 - deleting, 14-22
 - details page, 14-14
 - editing, 14-14, 14-19
 - exporting, 14-22
 - importing, 14-21
 - multi-bucket, 14-4, 14-16
 - search page, 14-11

- single-bucket, 14-3, 14-15
- status, 14-13
- transaction type, 14-13
- performance and activity, monitoring, 25-14
- performance monitoring, 20-1
- phrase, resetting, 4-19
- policies, 9-1
 - creating, 9-7, 9-11
 - deleting, 9-23
 - editing, 9-15
 - evaluating policy within a rule, 9-6
 - exporting, 9-25
 - importing, 2-7, 9-6, 9-25
 - linking to all users or a user ID group, 9-12
 - migrated from 10g to 11g, 9-25
 - nested, 12-5
 - planning, 9-6
 - search page, 9-8
 - searching for, 9-9
 - viewing, 9-9, 9-10
- policy, 0-xxxiv
 - management, 1-3
- Policy Details page, 9-10
- Policy Explorer, 5-4
- policy set, 11-1
 - details page, 11-2
 - editing, 11-6
- Policy tree, 3-9
- policy type, 9-6
- PostAuthScoring report, C-2
- PreAuthScoring report, C-2
- processPatternAnalysis, A-3
- properties
 - creating, 22-3
 - deleting database type properties, 22-4
 - editing the values for Database and File type, 22-3
 - exporting database and file type properties, 22-4
 - importing database type properties, 22-4
 - Oracle Adaptive Access Manager, D-1
- Properties Editor, using, 22-1
- purging, setting up, G-1, G-10, G-13

Q

- QA, 3-2
- QuestionStatistics report, C-2
- Quova file layout, 23-14

R

- RecentLogins report, C-1
- registration logic
 - configuring, 6-27
- registration phrase, 6-2
- registration questions, adding, F-5
- Registration report, C-2
- reporting, BI Publisher, 1-3
- reset
 - challenge questions, 4-22, 4-23, 6-7

- challenge questions and set of questions to choose from, 6-7
- challenge questions and the question set, 4-23
- customer, 4-4, 4-18
- customer profile, 4-22
- image, 4-18
- image and phrase, 4-20
- OTP, 8-3
 - profile, 8-8
- OTP profile, 4-20, 8-3
- phrase, 4-19
- virtual authentication device, 4-21
- reverse proxy integration, 1-5
- role permissions, CSR and CSR Manager, 4-5
- Routing Type group, 10-17
- routing types
 - group, 10-2
 - mapping, 23-15
- rule and fingerprint logging, I-1
- rule conditions
 - reference, B-1
- rules, 9-2
 - adding new, 9-16
 - creation process, 9-16
 - deleting, 9-32
 - details, 9-28
 - editing, 9-29
 - engine, 9-32, 12-5
 - preconditions, 9-30
 - results, 9-31
 - search page, 9-26
 - searching for, 9-27
- RulesAPIPerformance report, C-2
- RulesBreakdown report, C-3
- RulesPerformance report, C-2
- Run mode, 9-5

S

- SAML integration, 1-5
- scores, 12-1
 - and weight, 9-6
 - and weights, 9-32
 - calculations, 12-6
 - override
 - adding or deleting, 11-3
 - creating, 11-3
 - propagation, 12-4
- scoring engine, 9-6, 12-1, Glossary-12
- scoring override, 12-6
- ScoringCombinations report, C-3
- search for
 - challenge questions, 6-14
 - conditions, 9-33
 - groups, 10-5
 - policies, 9-9
- Search Results table, 3-13
 - menu and toolbar, 3-14
- searching for
 - rules, 9-27

- secondary authentication, 6-1
- Second-Level Domains group, 10-2, 10-11
- secret key for encrypting database values, 2-4
- secret keys, backup, 2-6
- security
 - administrator, 1-4
 - administrators, 3-2
 - effectiveness, monitoring, 25-15
 - investigator, 1-4
 - investigators, 3-2
- Session
 - Check Param Value, B-44
 - Check param value, B-3
 - Check param value for regex, B-3, B-45
 - Check param value in group, B-3, B-47
 - Check string param value, B-3
 - Check String Value, B-49
 - Check two string param value, B-3
 - Check value in comma-separated values, B-3
 - Compare two parameter values, B-3
 - Compare with current date time, B-3
 - Cookie mismatch, B-4
 - IP Changed, B-4
 - Mismatch in browser fingerprint, B-4
 - Time Unit, B-4
 - Time Unit Condition, B-49
- Session Details, 5-1
 - Checkpoint panels, 5-3
 - Login Details panel, 5-3
 - panels, 5-3
 - Transactions panel, 5-4
- sessions search, 5-1
- set up
 - KBA failure counter, 6-35
 - OTP, 8-3
 - OTP failure counter, 8-8
- single-bucket patterns, 14-3, Glossary-4
- snapshot
 - backup, 13-2, 13-5
 - best practices, 13-9
 - deleting, 13-7
 - details, 13-4
 - limitations, 13-7
 - metadata, 13-1
 - restore, 13-2, 13-6
 - search page, 13-3
 - storage, 13-1
- SOAP/Web services integration, 1-4
- State Confidence Factor, 9-31
- StateAggregates report, C-2
- States group, 10-2, 10-11, 10-12
- static linked (In Proc) integration, 1-4
- symmetric key to CSF, adding, 2-5
- synchronous actions, 15-8
- System - Check Boolean Property, B-4, B-52
- System - Check Int Property, B-4, B-52
- System - Check Model Maximum Score, B-4
- System - Check Model Minimum Score, B-4
- System - Check Request Date, B-4, B-54
- System - Check String Property, B-4, B-53

System - Evaluate Policy, B-4
system administrator, 3-2

T

tables in location loading, 23-18
tables used by the ETL process, 23-18
temporary allow, 4-3, 4-25
time zone, setting, 2-9, D-4
Top-Level Domains group, 10-3, 10-11
TrackerAPI Performance report, C-2
Transaction
 Check Count of any entity or element of a
 Transaction using filter conditions, B-4, B-35
 Check Current Transaction Using Filter
 Condition, B-26
 Check current transaction using the filter
 conditions, B-4
 Check if consecutive Transactions in given
 duration satisfy the filter conditions, B-37
 Check if consecutive transactions in given duration
 satisfy the filter conditions, B-4
 Check Transaction Aggregate and Count Using
 Filter, B-31
 Check transaction aggregate and count using filter
 conditions, B-4
 Check Transaction Count Using Filter
 Condition, B-27
 Check transaction count using filter
 conditions, B-4
 Check Unique Transaction Entity Count with the
 specified count, B-4
 Compare Transaction Aggregates
 (Sum/Avg/Min/Max) across two different
 durations, B-39
 Compare transaction aggregates
 (Sum/Avg/Min/Max) across two different
 durations, B-4
 Compare Transaction counts across two different
 durations, B-41
 Compare transaction counts across two different
 durations, B-4
 Compare transaction entity or element counts
 across two different durations, B-4
 Compare Transaction Entity/Element counts
 across two different durations, B-42
transaction, 16-1, 17-1
 data, 17-2
 definitions
 deactivating and activating, 17-12
 definition
 adding existing entity, 17-6
 definitions, 17-1, 17-2
 activating, 17-10
 create new entity to add, 17-7
 creating, 17-6
 defining source data, 17-8
 defining transaction data, 17-7
 deleting, 17-13
 editing, 17-11

 exporting, 17-11
 importing, 17-12
 mapping source data, 17-9
 viewing, 17-5
handling, 17-2
prerequisites for usage, 17-5
search page, 17-4
status group, 10-17
status groups, 10-3
transaction definitions, 1-3
trigger combination, 0-xxxiv
trigger combinations, 9-5, 9-19
trigger return combinations
 specifying, 9-21, 9-54
troubleshooting, 25-1

U

Universal Risk Snapshot, 13-1
unlock
 customer, 4-24, 8-3
 OTP, 4-21
 OTP user, 8-8
 user, 6-8
unregistering devices, 4-20
updateAuthStatus, A-3
updateTransaction, A-2
User
 Account Status, B-4
 Action Count, B-4
 Action Count Timed, B-5
 Action Timed, B-5
 ASN first time for user, B-5
 Auth Image Assigned, B-5
 Authentication Mode, B-5
 Challenge Channel Failure, B-5
 Challenge Failure, B-5
 Challenge Maximum Failures, B-5
 Challenge Questions Failure, B-5
 Challenge timed, B-5
 Check first login time, B-5
 Check information, B-5
 Check Last Session Action, B-5
 Check login count, B-5
 Check login time, B-5
 Check OTP failures, B-5
 Check User Data, B-5, B-55
 City first time for user, B-5
 Client and Status, B-5
 Country failure count for user, B-5
 Country first time for user, B-5
 Country first time from list, B-5
 Devices, B-5
 Distance from last successful login, B-5
 Distance from last successful login within
 limits, B-5
 Image Status, B-5
 In Group, B-5
 IP carrier first time for user, B-6
 Is last IP match with current ip, B-6

Is User Agent Match, B-6
Last login, B-6
Last login status, B-6
Location Used Timed, B-6
Login first time for user, B-6
Login In group, B-6
Login time between specified times, B-6
Max Cities, B-6
Max Countries, B-6
Max IPs Timed, B-6
Max Locations Timed, B-6
Max States, B-6
Multiple failures, B-6
Phrase Status, B-6
Preferences Configured, B-6
Question Status, B-6
Runtime score, B-6
Stale Session, B-56
Stale session, B-6
State first time for user, B-6
Status Count Timed, B-6
User Agent Percentage Match, B-5, B-6
User Group in Group, B-6
User is member of pattern N times, B-6
Velocity from last successful login, B-6
Velocity from last successful login within
limits, B-6
User ID group, 10-3, 10-13
Username group, 10-2, 10-13

V

vcrypt.tracker.autolearning.enabled, 2-9, 14-9
vcrypt.tracker.autolearning.use.auth.status.for.analysis,
2-9, 14-9
vcrypt.tracker.autolearning.use.tran.status.for.analysis,
2-9, 14-10
vcrypt.tracker.rules.allowControlledActions, 11-2
view
OTP performance data, 8-9
virtual authentication device, resetting, 4-21

W

weight, 12-1
Weighted Maximum scoring engine, 12-3
Weighted Minimum scoring engine, 12-3
Weighted scoring engine, 12-3