Oracle® Adaptive Access Manager

Concepts

Release 10*g* (10.1.4.5)

E12049-03

May 2009

Oracle Adaptive Access Manager Concepts, Release 10*g* (10.1.4.5)

E12049-03

Primary Author: Priscilla Lee

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

Contents

1 Introduction

2 Adaptive Strong Authenticator

3 Adaptive Risk Manager

4 Rules and Models

5 Auto-learning and Patterns

6 Transaction Definitions

7 Cases

8 Device Registration

Glossary

Index

Preface

Oracle Adaptive Access Manager Concepts introduces Oracle Adaptive Access Manager and describes the concepts required to understand and use the product effectively to fight against online identity theft.

Audience

This guide is intended for all users of Oracle Adaptive Access Manager, Oracle Identity Management's solution for web access real-time fraud detection and multifactor online authentication security for the enterprise.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

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

Related Documents

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

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

Conventions

The following text conventions are used in this document:

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

What's New

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

New Features for Release 10.1.4.5

These are the features introduced in the current release:

- Auto-learning

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

- Rule Template Editor

  The rule template editor allows the user to create and edit rule templates without having to go to the XML and write them.

- Configurable Actions

  Configurable Actions allow a user to create new supplementary actions that occur after the running of rules.

- Transaction Definitions

  Oracle Adaptive Access Manager provides a framework to support any kind of transaction by mapping client-specific data into the generic data model that supports the framework.

- Device Registration

  Device registration is a feature that allows a user to flag the computer, PDA or mobile phone he is using as a safe device. The customer can then configure the rules to challenge a user that is not coming from one of his registered devices. Device registration is available as a standard feature in Oracle Adaptive Access Manager. The feature can be turned on, although it is turned off by default in the product.

- Enumeration Editor

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

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

For an example of how the enumeration editor is used, refer to "Creating Runtimes" in the *Oracle Adaptive Access Manager Administrator's Guide*.

- Investigation tools

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

- Customizable reporting using BI Publisher

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

  Reports are editable through the BI Publisher. Column labels and contents can be editable. Also, aggregates and graphing can be added to reports.

- Globalization Support

  Oracle Adaptive Access Manager 10.1.4.5 has been translated into 26 languages for Adaptive Strong Authenticator and 9 for Adaptive Risk Manager. These translations are bundled along with the English version of the product.

- Conditions

  Rule conditions are the building blocks for constructing rule templates. Oracle Adaptive Access Manager includes a library of pre-configured conditions.

- Dashboard

  Adaptive Risk Manager includes a dashboard that provides performance and summary statistics as well as reports on locations, scoring, devices, security, and performance.

1 Introduction

When Internet fraud occurs, consumers and the enterprise lose. Online fraud is impacting our business in the following ways:

- Consumers are wary of legacy security's ability to prevent fraud
- Industry and government regulations are setting a higher standard
- Access management solutions do not have integrated strong security
- Stronger security without negative impact to user experience is needed
- Fraud costs business and consumers money

With the increasing sophistication of fraudsters and regulations governing online data privacy, organizations need a robust security solution.

- Stronger, adaptable security is needed for online applications
- Mutual authentication between site and user can prevent phishing
- Protect passwords and PINs from being stolen by malware
- More than a password is needed to protect users from attack
- Keep costs low and the complexity manageable in-house
- Deploy and integrate quickly without production delays

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.

Oracle Adaptive Access Manager (OAAM) is Oracle Identity Management's solution for web access real-time fraud detection and multifactor online authentication security for the enterprise. Oracle Adaptive Access Manager does not store any sensitive/meaningful data on the end user's machine (secure cookie and Flash object). Oracle Adaptive Access Manager also provides the customer flexible encryption options which are standards certified. Oracle Adaptive Access Manager uses 128 bit 3DES encryption (by default) for storing the KBA answers. But the encryption infrastructure is pluggable. E.g. Customer A can use 256 bit AES encryption if they choose.

Out-of-the-box, Oracle Adaptive Access Manager is designed to support complex, heterogeneous enterprise environments.

Delivering the next generation of risk-based evaluation, Oracle Adaptive Access Manager

- Enables real-time blocking of fraudulent access requests
- Delivers advanced alerting mechanisms

The product protects your business and your customers from a full range of attacks. Such types of attacks can include phishing, Trojans, viruses, fraudulent transactions, and Man-in-the-Middle attacks.

1.1 What Is Oracle Adaptive Access Manager?

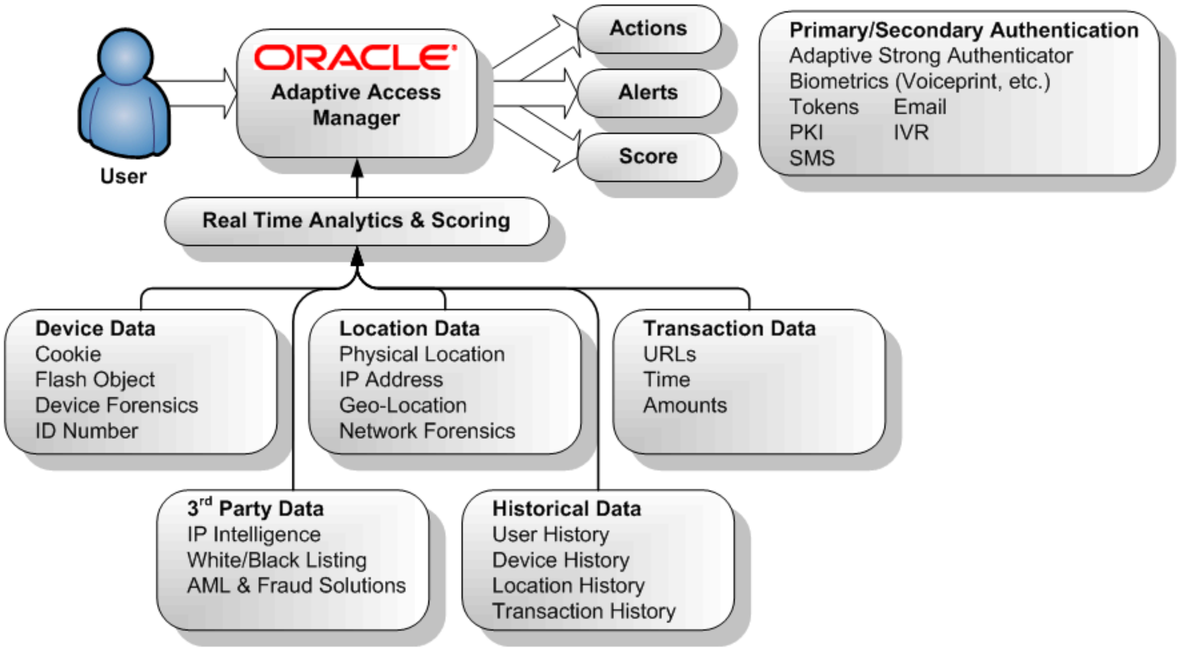
Oracle Adaptive Access Manager is a product to protect the enterprise and its customers online.

Oracle Adaptive Access Manager

- Provides multi-factor authentication security
- Evaluates multiple data types to determine risk in real-time
- Research and develop fraud policies in offline environment
- Integrates with access management applications

1.2 What Components Are Provided With Oracle Adaptive Access Manager

Oracle Adaptive Access Manager includes two core components. Adaptive Strong Authenticator includes a suite of highly secure virtual authentication devices. Adaptive Risk Manager works in real-time or offline to detect and prevent fraud.



1.2.1 What Is The Adaptive Strong Authenticator?

Adaptive Strong Authenticator is Oracle Adaptive Access Manager's user-facing "front-end" product with fraud protection against online Identity theft.

Oracle Adaptive Access Manager is an authentication agnostic security mechanism that incrementally protects sensitive credentials and data from phishing, pharming, trojans, and proxy-based fraud without the need for proprietary software downloads. It secures the data inputs at the point where they are first entered into an Internet browser; this ensures maximum protection because the raw information never resides on a user computer or anywhere on the Internet where it can be vulnerable to theft.

1.2.2 What Is The Adaptive Risk Manager?

Adaptive Risk Manager is Oracle Adaptive Access Manager's back-end, proactive real-time fraud detection product.

Adaptive Risk Manager provides a comprehensive anti-fraud software solution which works behind the scenes to provide second and third factors of security by verifying a host of factors used to confirm identity-from the computer and mobile device used to login to a user's location and online behavioral profiles. Based on these factors, Adaptive Risk Manager scores risk and alerts the organization of potential fraud in real-time. Adaptive Risk Manager can also trigger numerous actions, such as challenging or blocking the user.

The Adaptive Risk Manager comes with built-in web-based administration tools including Adaptive Risk Manager (Online and Offline), Customer Case Management, Security Monitoring, Reporting, and System Administration functionality.

1.2.2.1 What Is The Adaptive Risk Manager Online?

Adaptive Risk Manager Online is the administration and monitoring user interface of Oracle Adaptive Access Manager. It is used to configure and monitor the system in real-time, as well as run reports on the Adaptive Risk Manager database.

Adaptive Risk Manager Online provides sophisticated fraud monitoring, analysis, and tracking by user location, device, time of day, type of transaction, as well as a host of other factors, and evaluates these factors against a set of customizable rules.

1.2.2.2 What Is The Adaptive Risk Manager Offline?

Adaptive Risk Manager Offline is an offline fraud analysis product that evaluates existing transaction data for two main purposes:

- First, Adaptive Risk Manager Offline can be used as a stand alone security tool to analyze, detect and alert high risk transactions.
- Secondly, Adaptive Risk Manager Offline can be used in conjunction with Adaptive Risk Manager Online as a supplemental offline analysis tool and as a way to pre-visualize rules against real customer data without impacting customers in a real-time environment.

2

Adaptive Strong Authenticator

Common authentication methods today have many weaknesses:

- Data remains raw between the point of creation and where the encryption process is invoked. Moving raw data over open lines increases the opportunity for theft.
- Every protection implemented on a data source depends on a human being to maintain its state of security, which can be compromised.
- Any new computing environment can be well-studied and misused because of its predictable behavior.

Oracle Adaptive Access Manager's Adaptive Strong Authenticator was designed specifically to overcome these limitations.

Leveraging a soft, two-factor authentication solution, Adaptive Strong Authenticator provides fraud protection against online identity theft. It does so by encrypting credential data inputs at the point of entry. This ensures maximum user protection because information never resides on a user's computer nor does information reside anywhere on the Internet where it can be vulnerable to theft.

2.1 Protecting Corporations and Their Customers

As corporations embrace the Internet, they must ensure that customer transactions and data are safe. Adaptive Strong Authenticator enables corporations to deploy a highly effective security solution that offers their customers the required protection as well as the ease-of-use needed to engage in and grow online relationships.

Adaptive Strong Authenticator is hardware- and software-independent and does not rely upon cached data. End-users can invoke the authentication process from any browser, over any network (public, private, Wi-Fi, and kiosk). They can also use any user touch-point to protect their information during session initiation or during in-session transactions.

Low Cost of Ownership

An added benefit of Adaptive Strong Authenticator is that it offers a low cost of ownership. This is in comparison to other authentication alternatives. The solution does not require any special databases, proprietary software, extra hardware, or third-party servers. Furthermore, there are no customer support needs to consider associated with lost or damaged cards and tokens.

Using Adaptive Strong Authenticator, corporations can defend their customers and their data against the most potent fraudulent attacks.

Table 2–1 Potent Fraudulent Attacks

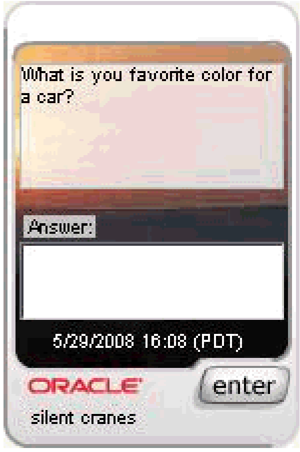
Attack	Defense
Phishing Environment	The PIN data required to authenticate only exists in a form understood by the user and the server. Therefore, it can't be interpreted and used for fraud. An impostor Internet site cannot simulate the operational aspects of the authentication.
Phishing (Social Engineering)	Equipping end-users with their own personalized device is the first step. Ensuring Adaptive Strong Authenticator is used for entry of all sensitive credentials (password, PIN, challenge questions, and others) is the second. Finally, Adaptive Risk Manager prevents the fraudulent use of credentials if end-users have fallen prey to phishing.
Trojan Viruses	Adaptive Strong Authenticator foils keyboard, mouse-click, and screen-capture loggers; cookie hijackers; "over the shoulder" spies; and all other forms of known attacks. This is because no sensitive data is entered using the keyboard, mouse, or cookies nor is any sensitive data handled by the browser.
Fraudulent Transactions	Adaptive Risk Manager collects and evaluates end-user data points. These data points can be used to authorize, challenge, deny, or put online transactions on hold.
Password Theft	Adaptive Strong Authenticator generates a unique set of random data for every user session. It is virtually difficult for a password to be guessed and reused.

2.2 Comprehensive Features and Functionality

Adaptive Strong Authenticator is an enterprise-licensed platform that includes a number of user interfaces. These interfaces are for managing fraud and identity theft protection. Whether making payments, accessing sensitive documents, entering passwords, or answering challenge questions, users and data are protected.

2.2.1 QuestionPad

QuestionPad takes data entry to another security level. With challenge questions becoming more commonly used in financial institutions and other enterprises, it opens up another target for fraudsters. QuestionPad addresses this issue by changing the way users enter these new credentials.

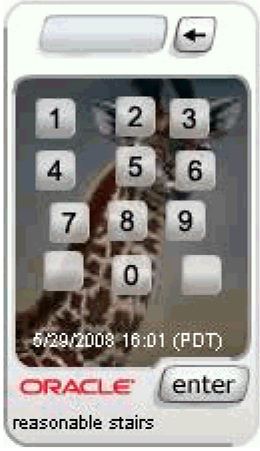


What is you favorite color for a car?

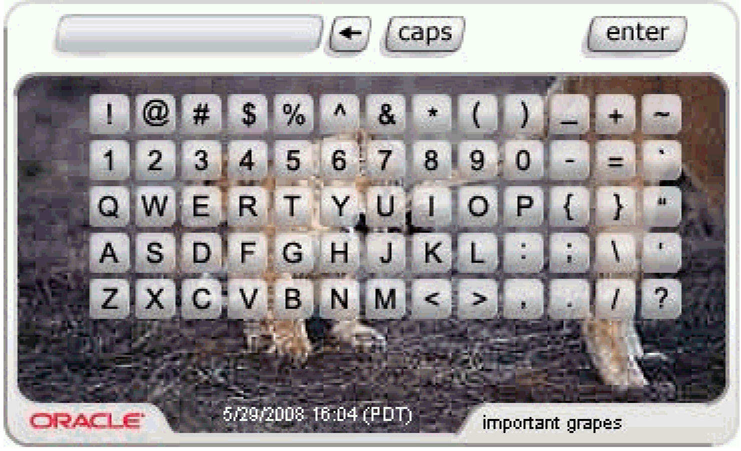
QuestionPad offer several deployment options. Oracle can host the challenge questions and provide the question bank. Alternatively, the question bank can be integrated with internal customer information databases. They can also be integrated with external third-party question providers.

2.2.2 PinPad and KeyPad

PinPad is an authentication entry device used to enter a numeric PIN. It can be invoked at the time of login or transaction.

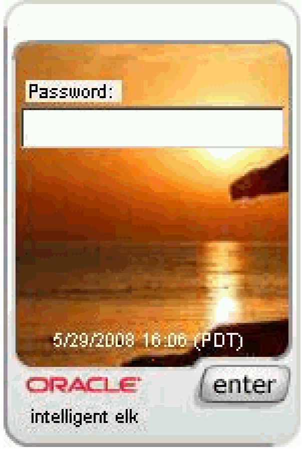


KeyPad is a configurable virtual keyboard. It can be used to enter alphanumeric and special characters found on a traditional keyboard. That makes it ideal for entering passwords and other sensitive alphanumeric information.



2.2.3 TextPad

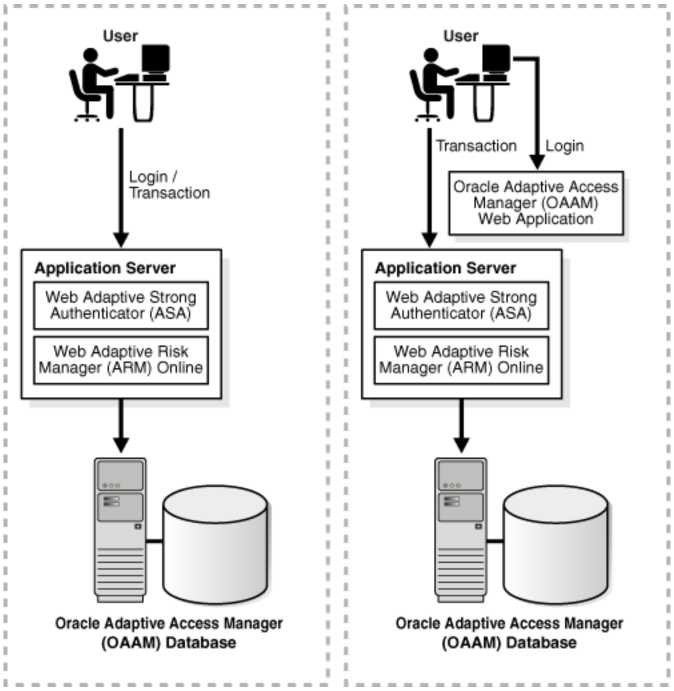
TextPad is a personalized device for entering a password or PIN using a regular keyboard. This method of data entry helps to defend against phishing.



2.3 Deployment Options

Two deployment options are available:

- Without Oracle Adaptive Access Manager Web Application
- With Oracle Adaptive Access Manager Web Application


User
Login / Transaction
Application Server
Web Adaptive Strong Authenticator (ASA)
Web Adaptive Risk Manager (ARM) Online
Oracle Adaptive Access Manager (OAAM) Database
User
Transaction
Login
Oracle Adaptive Access Manager (OAAM) Web Application
Application Server
Web Adaptive Strong Authenticator (ASA)
Web Adaptive Risk Manager (ARM) Online
Oracle Adaptive Access Manager (OAAM) Database

2.3.1 Without Oracle Adaptive Access Manager Web Application

With this deployment approach, the client stores all credentials. The client also uses the Adaptive Strong Authenticator library only for encoding and decoding inputs.

2.3.2 With Oracle Adaptive Access Manager Web Application

With this deployment approach, customers can configure their own Web interface. They do this by leveraging packaged Web pages and flows from Oracle. These pages and flows can then be altered to meet corporate branding requirements.

3

Adaptive Risk Manager

Adaptive Risk Manager, a core component of Oracle Adaptive Access Manager, enables an enterprise to evaluate and score risk. It can do so for each online login and transaction. As a result, the solution increases authentication security in real-time for high-risk situations.

Adaptive Risk Manager provides a strong second- and third-factor of security for the enterprise. It can serve as a standalone solution that offers increased security, with no change to the user experience, and it can also be used in combination with Adaptive Strong Authenticator. Together the components provide further anti-identity theft and fraud protection.

3.1 Multiple Factor Risk Protection

Adaptive Risk Manager verifies each user's computer and location ("something you have"). It also verifies a user's behavior patterns to confirm identity ("something you are"). These verifications are added to existing enterprise requirements for login/password credentials and additional knowledge-based authentication ("something you know"). This offers the enterprise multiple strong factors of antifraud protection.

Adaptive Risk Manager uses dozens of "tentacles," including proprietary one-time use secure cookies, Flash objects, and other patent-pending technologies. These serve to recognize and fingerprint the device you typically use to log in to your computer, laptop, a kiosk and so on. In this way, Adaptive Risk Manager makes your personal computer your second factor-without requiring any change in your behavior.

Also patent pending is the unique process used for device fingerprinting. It is a process that creates a fingerprint good for use one-time only. Therefore, it is immediately invalidated if a fraudster attempts to reuse it.

Adaptive Risk Manager evaluates the pre-, post-, and in-session characteristics of each transaction. This ensures fraud detection and transactional integrity.

The solution's proprietary, real-time device and location fingerprinting can determine whether a login attempt is high risk. Prior to authentication, these determinations are made with a high probability. Subsequently, each individual transaction attempted in session is further scored for risk, resulting in an even higher level of confidence for the user.

Adaptive Risk Manager then governs the institution's response to risk, whether it is an alert, user challenge, or secondary authentication. This is done in real-time using Adaptive Strong Authenticator.

3.2 Comprehensive Features and Functionality

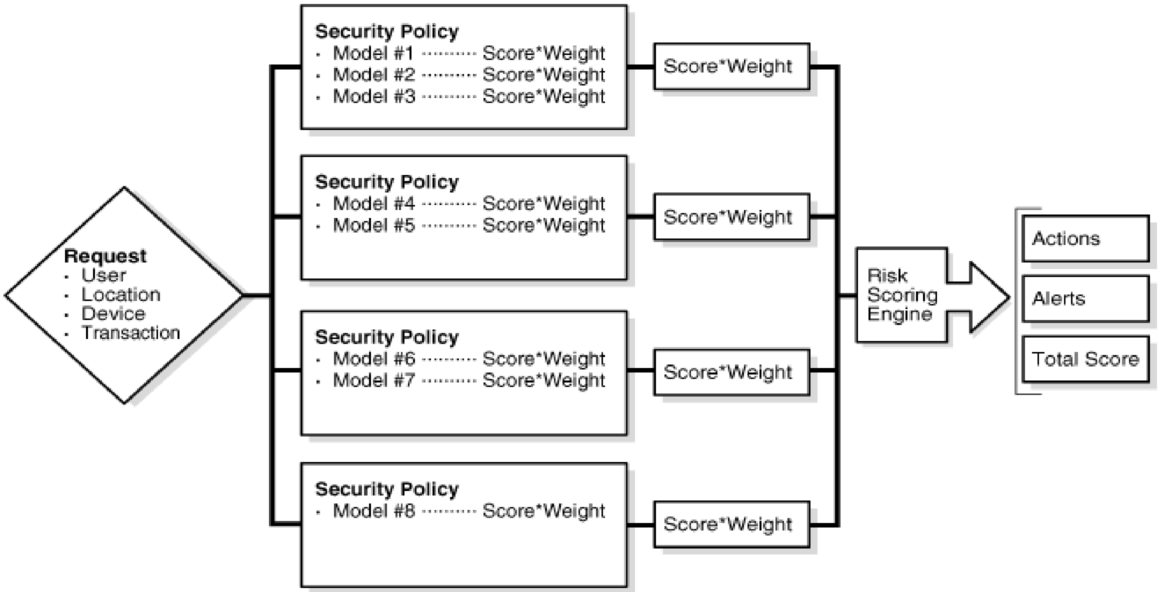
Adaptive Risk Manager is an open, standards-based system. It is available as a single-server installation or a cluster of servers that can be integrated with existing enterprise Web applications using prepackaged APIs.

Adaptive Risk Manager includes the following standard features:

- **An Engine**. State-of-the-art, real-time rules and risk-scoring is provided.
- **Integration support.** Third-party integration is supported via open APIs and shared authentication and fraud services infrastructure.
- **Proprietary fingerprinting**. Patent-pending fingerprinting methods for device, location, and workflow use second and third factors for identification.
- **Models and rules.** Customizable scenarios invoke any set of rules. They are driven entirely by the needs of the organization and the level of security defenses required.
- **Administration tools.** Comprehensive user interfaces are provided to maximize leverage and usage of the application. This includes dashboards, reports, and modeling tools.

3.2.1 Adaptive Risk Manager Engine

The Adaptive Risk Manager engine offers state-of-the-art, real-time rules and risk scoring. The robust engine combines analytics, including states, rules, and pattern recognition. This ensures intelligent real-time operations and maximum enterprise protection against online fraud.


Request
· User
· Location
· Device
· Transaction
Security Policy
· Model #1 ·········· Score*Weight
· Model #2 ·········· Score*Weight
· Model #3 ·········· Score*Weight
Security Policy
· Model #4 ·········· Score*Weight
· Model #5 ·········· Score*Weight
Security Policy
· Model #6 ·········· Score*Weight
· Model #7 ·········· Score*Weight
Security Policy
· Model #8 ·········· Score*Weight
Score*Weight
Score*Weight
Score*Weight
Score*Weight
Risk Scoring Engine
Actions
Alerts
Total Score

Adaptive Risk Manager analytics are designed for high performance and scalability. The Adaptive Risk Manager engine works by automatically preanalyzing policies (sets of modules) and models (sets of rules). Then it actively monitors each user's transactional data flows to identify those elements that might impact the models.

The Adaptive Risk Manager engine uses a proprietary structure to simultaneously maintain the necessary parameters. It then updates and tests them against the relevant models.

3.2.1.1 Rules Engine

The Adaptive Risk Manager engine triggers actions and alerts based upon rules. These rules are housed in models configurable by the institution and are established according to the institution's policies:

- Security policies (pre- and post-authentication)
- Fraudster rules (subset)
- Transaction policies (in session)
- Third-party data

Security policies (pre- and post-authentication)

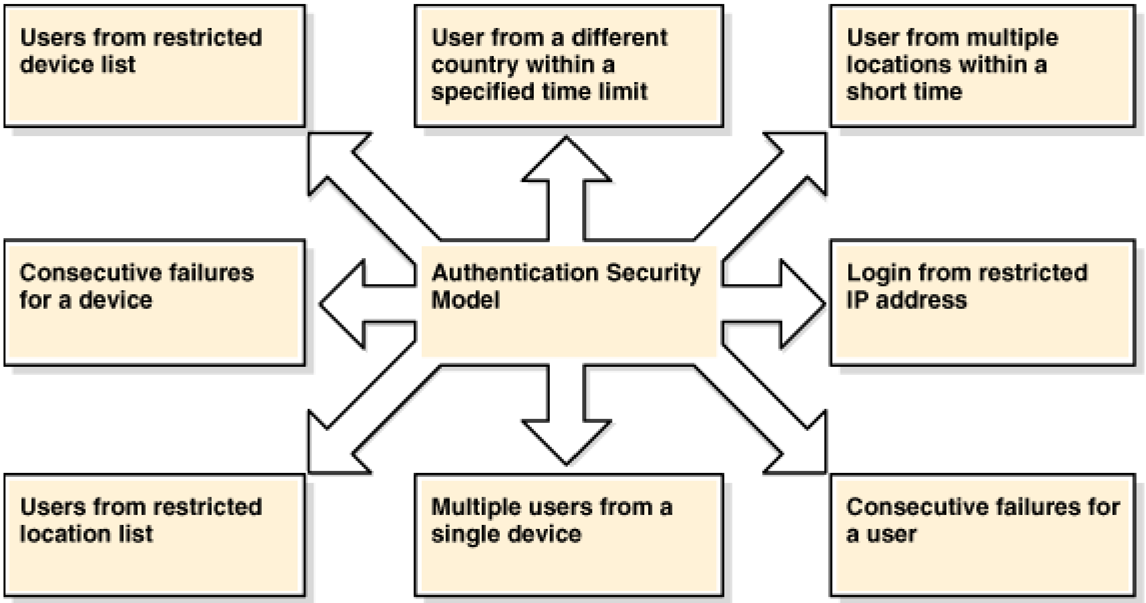
Security policies use standards for detecting fraudster behavior developed from cross-industry best practices:

- Anomaly detections
- Misuse detections
- Intrusion detections
- Predefined fraudster models (the figure shows a subset of the fraudster rules that are standard in Adaptive Risk Manager)
- Customizable models

  Adaptive Risk Manager's extensive fraudster models are enriched by Oracle's cross-industry customer base. Its customer base covers financial services, e-commerce, health care, and the military, among others.

Fraudster rules (subset)

Fraudster rules are a collection of some basic anti-fraud rules.


Users from restricted device list
User from a different country within a specified time limit
User from multiple locations within a short time
Consecutive failures for a device
Authentication Security Model
Login from restricted IP address
Users from restricted location list
Multiple users from a single device
Consecutive failures for a user

Transaction policies (in session)

Transaction policies invoke rules based upon parameters established by the business for mitigation of transaction risk, including

- In-session transaction monitoring

- Business-defined transaction rules
- Key value-driven logic
- Customizable models

Third-party data

Third-party data offers prepackaged integration with third-party data providers, developed through Oracle's strategic partnerships. Thus, third-party data can be called and evaluated in Adaptive Risk Manager as part of the risk score:

- IP intelligence
- Risk data
- Historical data (data warehouse)
- Customer data

3.2.1.2 Risk Scoring/Forensics

Adaptive Risk Manager risk scoring is a product of numerous fraud detection inputs such as a valid user, device, location, or pattern. Also included are third-party data and historical customer data. These inputs are weighted and analyzed in real-time within Adaptive Risk Manager's fraud analytics engine.

Design

Adaptive Risk Manager's design features are listed below:

- Customer models/rules.

  Any custom rule can be set, according to business need, to become activated if a transaction is scored above a certain risk threshold.

- Nested models.

  Nested models can be assigned to ensure a higher degree of accuracy for the risk score. A nested model is a secondary model. It is used to further quantify the risk score in instances where the original result output by the system is inconclusive. A nested model is run only when a specific sequence of answers is returned from the primary model. Nested models therefore reduce false positives and negatives.

3.2.1.3 Real-Time Response

Adaptive Risk Manager is configured, based upon rules, to initiate a response to an elevated risk score (see "Models and Rules"). Responses are documented below.

Internal flag/watch list

Internal flag/watch list is used for follow-up investigation within the institution.

Secondary Authentication - Out of Band

One-Time-Password (OTP) through Interactive Voice Response (IVR) is available from our partners.

Secondary Authentication - Online

- Challenge questions.

  Adaptive Strong Authenticator can be used to provide further defenses against in-session attacks. It can also enable "weakest link" security by protecting the challenge/response process.

- Tokens, smart cards, identity proofing, and so forth (available from partners).

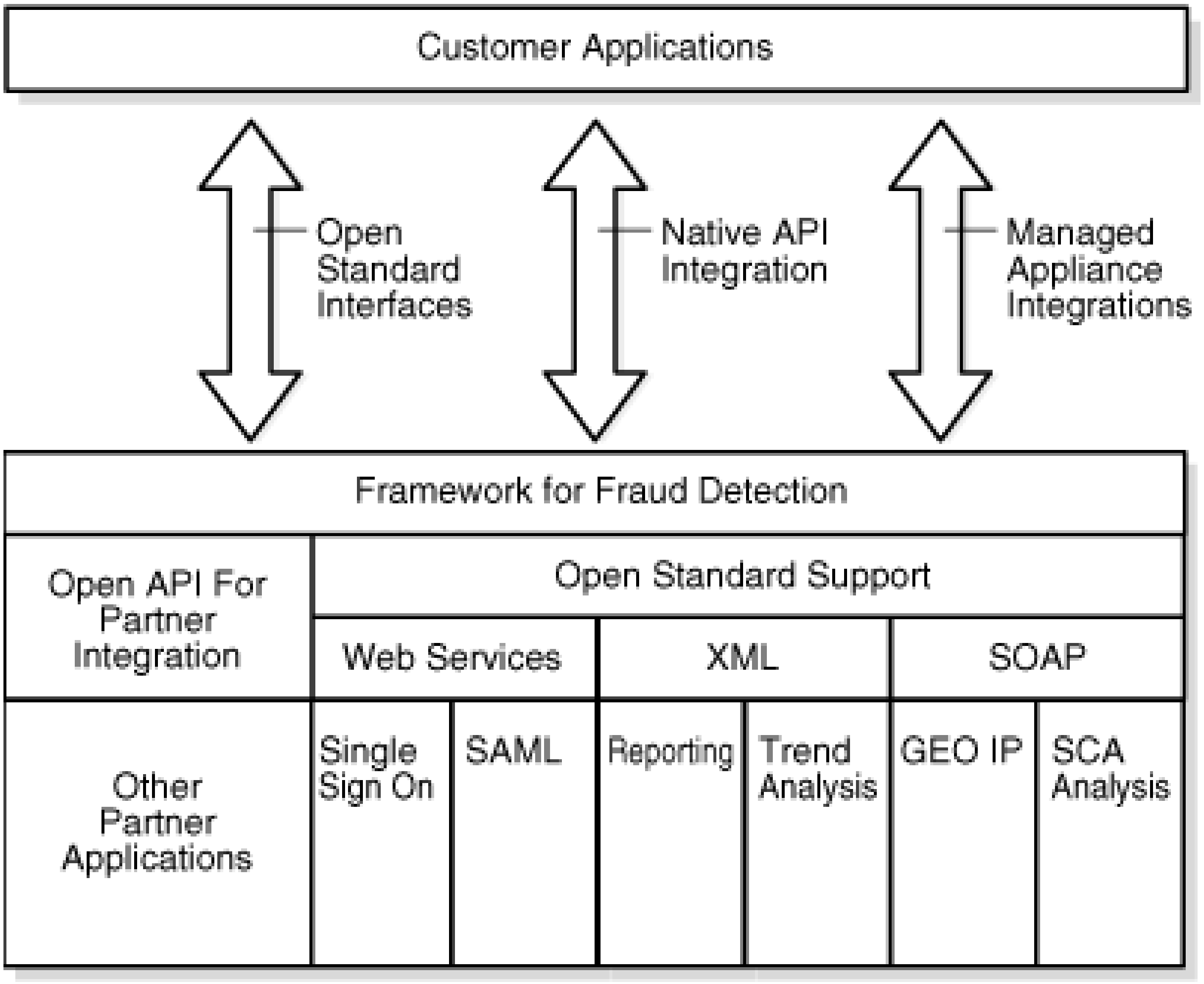
3.2.2 Integration Advantages

Adaptive Risk Manager is an open, standards-based platform. It is designed for minimal integration work and maximum compatibility with existing enterprise and third-party systems. Adaptive Risk Manager features best-of-breed integration capabilities that enable the institution to speed up and simplify its deployment. These capabilities also enable the institution to leverage data from external systems for Adaptive Risk Manager.

Oracle Adaptive Access Manager is standard J2EE WAR. It doesn't have EJB component and supports all standard J2EE servlet containers out of the box. There is no special configuration required on the container side, except setting the JNDI and Access Control Roles using the container provided mechanism.

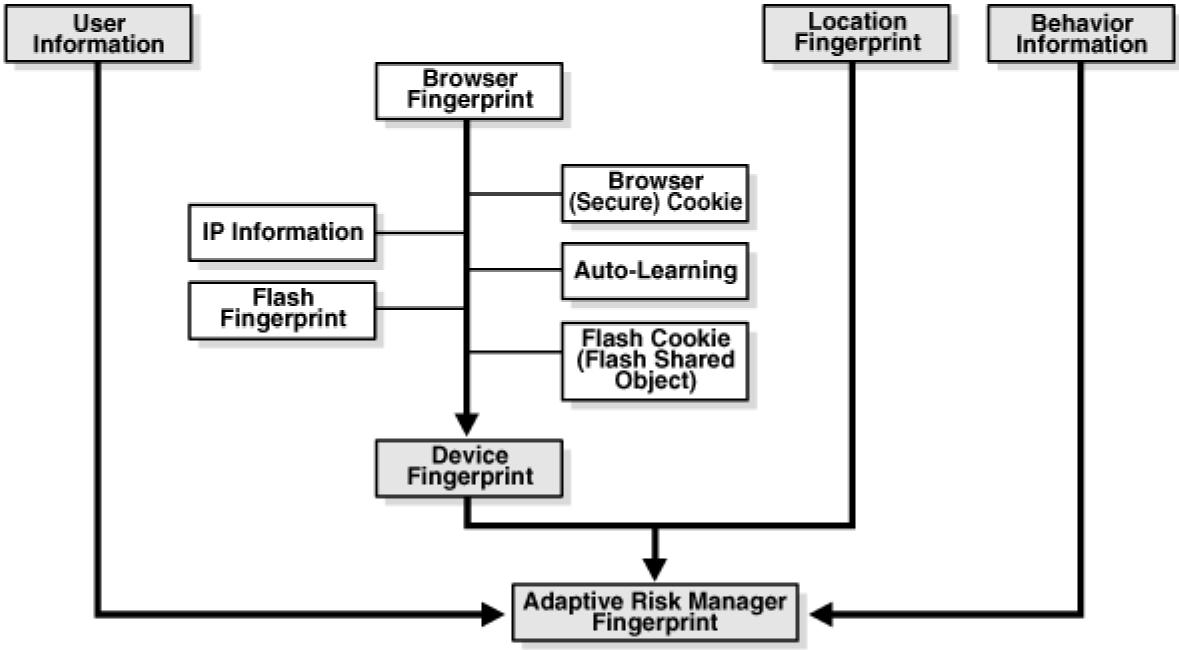
Oracle Adaptive Access Manager provides generic groups, which can be populated with external data and can be used in the rules engine. The rule engine itself is JSR94 compliant and can be used to write customized rules. Additionally, it provides interface classes, which can be overwritten to extend the product (configurable action infrastructure to support custom rule actions, configurable Adaptive Strong Authenticator web application for supporting complex integration, encryption algorithm options, etc.).

A list of prepackaged APIs is available in the current version of Adaptive Risk Manager. APIs are available in the areas of Active Directory, Lightweight Directory Access Protocol, fraud, Annotation Markup Language, customer relationship management, Single Sign-On, compliance, and mainframe systems.



3.2.3 Proprietary Fingerprinting

Much of Adaptive Risk Manager's power lies is in its patent-pending fingerprinting methods for device and location. Adaptive Risk Manager stores and uses multiple second and third factors to establish these fingerprints. The figure below shows a partial list. Additions are ongoing via industry partnerships and Oracle's own research and development.



3.2.3.1 Device

Adaptive Risk Manager monitors a comprehensive list of device attributes. If any attributes are not available the device can still be fingerprinted.

Adaptive Risk Manager's patent-pending method for device fingerprinting generates a one-time fingerprint for each user session. That fingerprint is unique to the individual's device. It is replaced upon each subsequent visit with another unique fingerprint. This ensures that a fingerprint cannot be stolen and reused for fraud

For 10.1.4.5, a device registration feature is available that allows a user to flag the computer he is using as a safe device. The customer can then configure the rules to challenge a user that is not coming from one of his registered devices. Device registration is available as a standard feature in Oracle Adaptive Access Manager. The feature can be turned on, although it is turned off by default in the product.

3.2.3.2 Location

Adaptive Risk Manager contains sophisticated location fingerprinting capabilities. A blend of IP intelligence data is used to identify locations by geography and many other data points crucial to accurate fraud detection.

3.2.3.3 Multilevel Security

The benefits of Adaptive Risk Manager fingerprinting and risk scoring are cumulative. Device and location fingerprints are already verified by the time a user attempts a transaction in session. Thus, Oracle Adaptive Access Manager achieves an additional level of confidence.

To further enhance Oracle's proprietary methods, Adaptive Risk Manager also features prepackaged integration with partners. These partner solutions also monitor the customer experience at the individual user level.

Third-party data can be fed into the Adaptive Risk Manager analytics engine as part of the fingerprint. This enhances the overall picture of customer activity.

3.2.3.4 Auto-learning

Auto-learning, a feature available in the 10.1.4.5 release, is a profiling process in which Adaptive Risk Manager identifies behavior patterns (buckets) based on the parameters the administrator specifies. Adaptive Risk Manager then automatically records/maintains the bucket memberships of the users/devices/locations (entities in general) over time so that the data that is gathered can be used as a way to evaluate risk.

3.2.4 Models and Rules

Institutions can deploy Adaptive Risk Manager in a variety of customizable scenarios to invoke any set of rules. These rules are driven entirely by the needs of the institution and the level of security required. Rules can also be applied in any combination to different segments of users. This can be done in any way the institution wants to segment its user population.

As previously discussed, Adaptive Risk Manager monitors and evaluates activity by four main criteria: user, device, location, and workflow. Each criterion contains various pieces of Adaptive Risk Manager data. That data is used to detect fraud risk (and, optionally, data seamlessly integrated from third parties as well).

Within Adaptive Risk Manager, data is organized into groups corresponding to these criteria. These groups are then linked to compatible models containing rules used to evaluate activity.

Over time, there are several ways the institution can continue to expand and develop the models. For more information about Rules and Models, refer to Chapter 4, "Rules and Models."

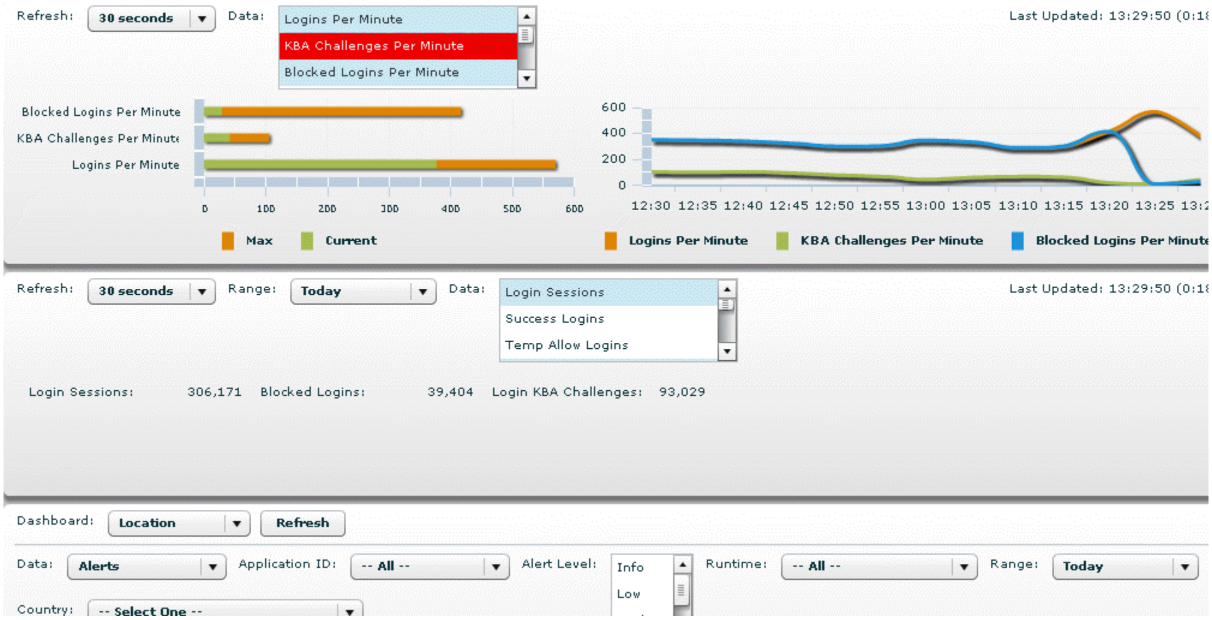
In 10.1.4.5, a Rule Template Editor feature is available that allows the user to create and edit rule templates without having to go to the XML and write them.

3.2.5 Comprehensive Administration Tools

Comprehensive user interfaces are a standard part of Adaptive Risk Manager to help the institution leverage the system.

3.2.5.1 Dashboard

The dashboard provides real-time visibility into potential fraudulent activities. It provides performance and summary statistics as well as reports on locations, scoring, devices, security, and performance. These help analyze online traffic; identify suspicious behavior; and design rules for proactive fraud prevention, risk monitoring, and case management.



Refresh: 30 seconds

Data: Logins Per Minute / KBA Challenges Per Minute / Blocked Logins Per Minute

Last Updated: 13:29:50 (0:1

Refresh: 30 seconds

Range: Today

Data: Login Sessions / Success Logins / Temp Allow Logins

Last Updated: 13:29:50 (0:1

Login Sessions: 306,171 Blocked Logins: 39,404 Login KBA Challenges: 93,029

Dashboard: Location

Data: Alerts

Application ID: -- All --

Alert Level: Info / Low

Runtime: -- All --

Range: Today

Country: -- Select One --

Performance and Summary

The performance and summary panels provide views of statistics on the current rate of logins and an overview of activity. This includes login sessions, successful logins, blocked logins, alerts, rules triggered, and rules run.

Dashboards

The dashboard panel provides access to five dashboard types: Location, Scoring, Device, Security, and Performance. The dashboard offers a real-time view of the secured site. It delivers a high-level personalized business view of the current status of user behavior and key transactions.

- Location

  Location provides aggregated location statistics including location, device, and users detected.

- Scoring

  Scoring displays statistics on risk score, runtime, and the number of sessions.

- Devices.

  Device provides statistics on the browser, OS, number of sessions, and percent of total.

- Security

  Security displays statistics on alerts that were run during the time frame, including runtime; alert level and type; and information on rules that were run during the time frame, such as model, runtime, action, and count.

- Performance

  Performance displays statistics on models, rules, actions, and APIs performance.

3.2.5.2 Reports

Oracle Adaptive Access Manager's comprehensive reporting area contains reports to assist with enterprise-level and individual customer-level fraud management. The reports enable detailed risk management and analysis through drill-down capabilities for viewing information. Such views are by location, device, user, and transactions over specific time ranges and schedules. Reports are editable through the BI Publisher. Column labels and contents can be editable. Also, aggregates and graphing can be added to reports.

3.2.5.3 Configurable Actions

Configurable Actions allow a user to create new supplementary actions that occur after the running of rules.

3.2.5.4 Transaction Definitions

Oracle Adaptive Access Manager provides a framework to support any kind of transaction by mapping client-specific data into the generic data model that supports the framework.

3.2.5.5 Enumeration Editor

Starting in the 10.1.4.5 release, existing enumerations and their elements and properties can be edited in Adaptive Risk Manager. New enumerations can also be created to customize Adaptive Risk Manager.

3.2.5.6 Investigation Tools

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

4 Rules and Models

This chapter provides detailed information on Adaptive Risk Manager's Rules and Models.

4.1 Overview

Adaptive Risk Manager, a core component of Oracle Adaptive Access Manager, enables an enterprise to evaluate and score risk. Oracle Adaptive Risk Manager uses "Rules" to evaluate the traffic running through the system. At Runtime, the specified points in a session where Adaptive Access Manager collects incoming data, and the Rules are run. If the data is evaluated and the specified conditions of the Rule are met, the Rule triggers and a final outcome, such as an action, an alert, or a total score results.

Examples of Runtimes are bill payment, wire transfer, execute trade, request document, and so on.

An Example

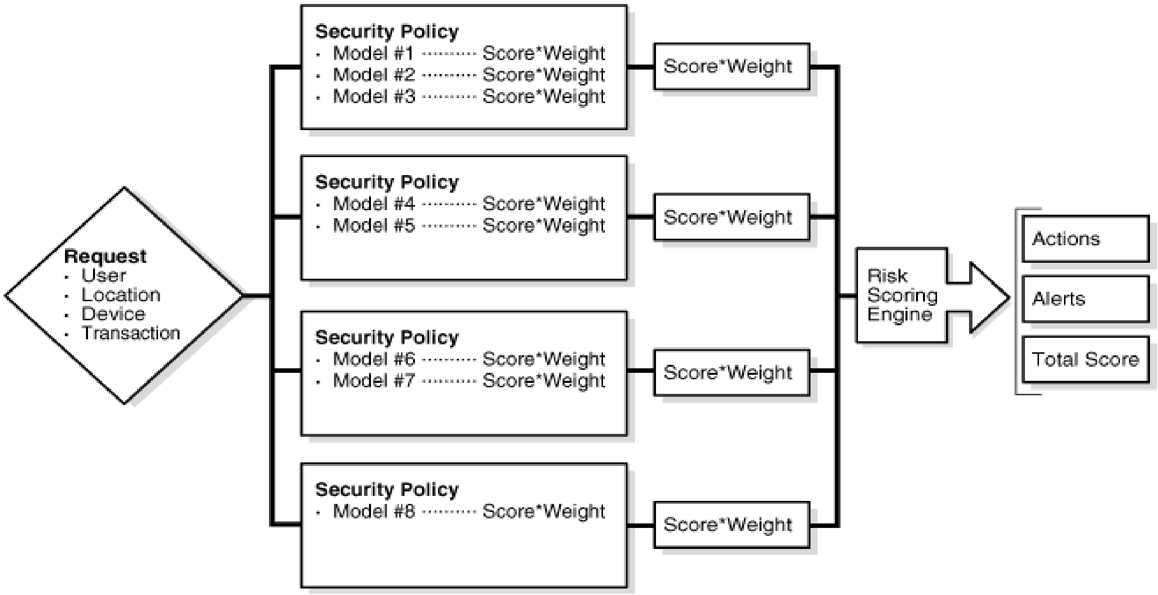
If an online grocery store is concerned with customer logins and grocery purchases (two Runtimes), it may create its own grocery Model and customize a set of Rules for this Model.

The grocery store then configures the Rules to trigger during the points in time (customer logins and grocery purchases).

Data is collected and evaluated by Adaptive Risk Manager for possible fraud. If the preconditions set for possible fraud are matched, and the conditions driven by the Rule Template are met, the Rule is triggered.

Based on how the grocery store has configured what it wants for an outcome, an action, an alert, or a total score may result.

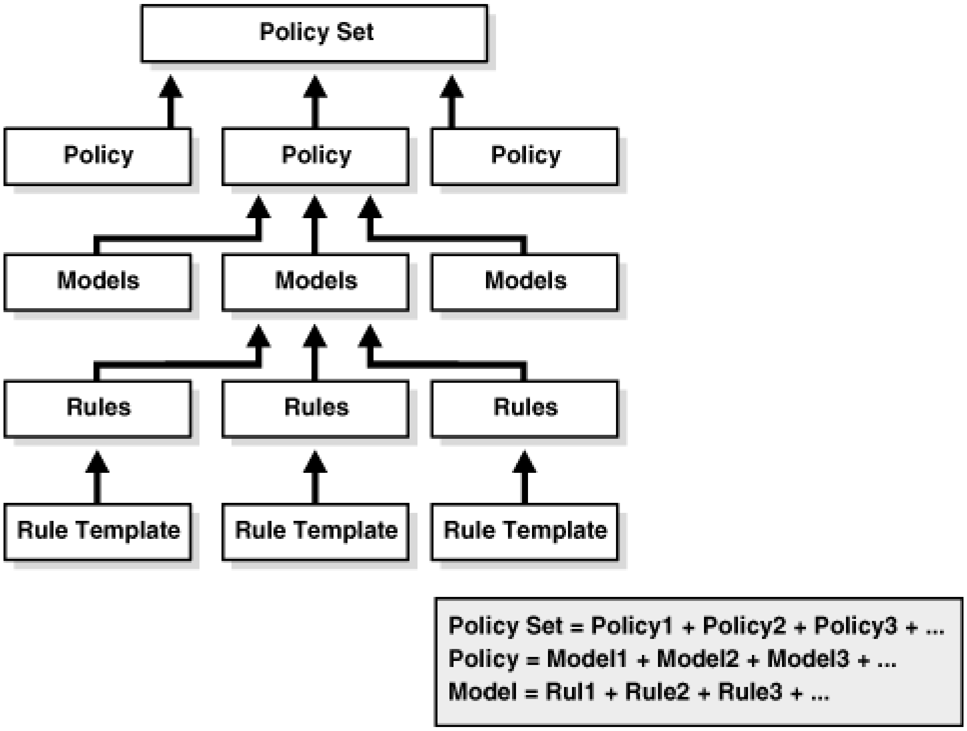
The following illustration shows how the Risk Scoring Engine determines actions, scores, and alerts based on Policy.



4.2 Concepts and Terminology

Concepts and terminology for Rules and Models are provided below.

The following illustration shows the relationship between Rule Templates, Rules, Models, and policies.

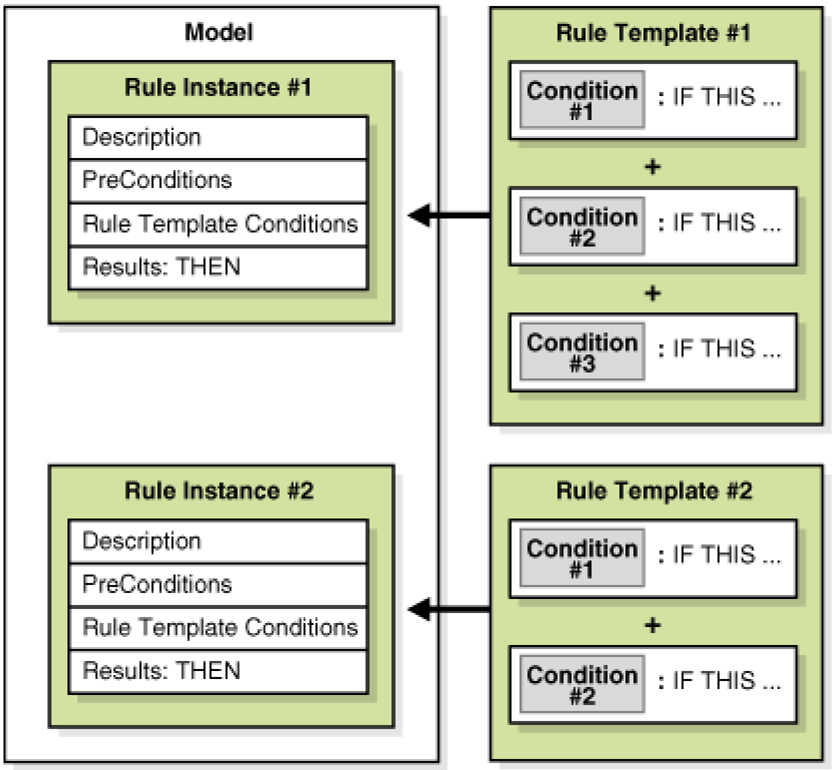

Policy Set
Policy
Policy
Policy
Models
Models
Models
Rules
Rules
Rules
Rule Template
Rule Template
Rule Template
Policy Set = Policy1 + Policy2 + Policy3 + ...
Policy = Model1 + Model2 + Model3 + ...
Model = Rul1 + Rule2 + Rule3 + ...

4.2.1 Rule Conditions/Rule Templates

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

The rule template forms the basis for creating a rule instance. Adding condition instances to rule templates allow you to create the template you need for your use cases. Rule templates must have at least one condition. After you configure a rule template, attach the rule instance to a Model and load it into memory, the rule instance is ready to execute against client data to check fraud activity.

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



4.2.2 Rules

A Rule describes an operation that identifies and reacts to certain information that may indicate fraud.

Rules are housed in Models within a certain Policy and trigger actions, alerts, and scores

A Rule is configured so that it can evaluate the risk involved with the incoming user traffic for specific groups of users or all users accessing the system and trigger an action, an alert, or a final score when all pre-conditions set by the administrator and conditions specific to and driven by the Rule are met.

Each Rule has a name and a valid description. The Rule instance is part of a specific Model and cannot be reused.

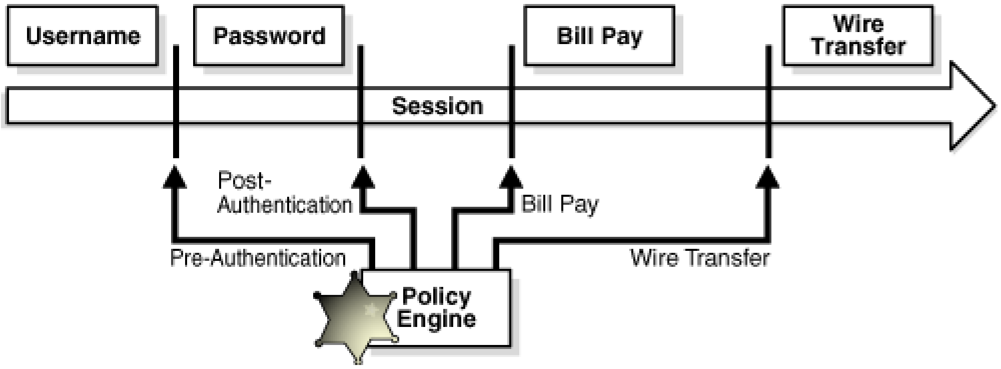
The Rule instance has four basic components:

Table 4–1 Rule Instance Components

Component	Description
Rule Name and Description	The name and description of the Rule instance.
Preconditions	Preconditions must be met before continuing on to the actual Rule conditions.
Conditions	Conditions are specific to the Rule Template. This Conditions section is completely determined by the Rule Template and looks different for the different Rule Templates.
Results	Results are desired outcomes have been specified to occur when the Rule conditions are met.

4.2.3 Runtime

A Runtime is a specified point in a session when rules in a model will run. For example, at pre-authentication, post-authentication, and in-session. Risk can be evaluated at any time specified by a Runtime.



To gain access to sensitive data or transactions a user must successfully pass through multiple security checkpoints.

4.2.4 Action

An action is always used in Rules to specify steps/actions to take for the client application. Standard actions like block, allow, challenge, and others are provided out-of-the-box.

These actions are specified in configuration files and can be added or removed at configuration time.

4.2.5 Alert

Alerts are generated by the Rules Engine and typically used for customer care, fraud, and investigational purposes. The Adaptive Risk Manager can also be configured to send alert emails.

The Adaptive Risk Manager provides an interface to view alerts.

4.2.6 Post Process

The post process is used to determine the final action for the multiple actions that result from Rule processing. Post processing is performed at deployment time using configuration files.

4.2.7 Group

A Group is a collection of related entities that the client wants to monitor.

Examples of different groups are:

- User
- Location (cities, states, countries, IPs, IP ranges, etc.)
- Device
- Action (block, challenge, allow, etc.)
- Alerts (different messages)

4.2.8 Action Group

An action group is a group of actions and contains zero or more actions. An action group is typically used to indicate all the actions that need to occur when the Rule is triggered.

4.2.9 Alert Group

An alert group is a 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.

4.2.10 Score

Score refers to the numeric scoring used to represent the risk level associated with a specific situation. A score is an integer value from 0 to 1000 and one of the outputs for the client application. Models can be configured to generate various scores that a client application can act upon.

4.2.11 Weight

Weight refers to the multiplier value applied to the score used to influence the total score at various evaluation levels. The weight is how this Model score is to be weighed compared to other Models in same Policy Type. Weight is only used when a given Policy Type is using a "weighted" Scoring Engine.

Weight is an integer value from 0 to 100.

4.2.12 Risk Score

Risk score is a component of numerous fraud detection inputs, which are weighted and analyzed in real time within Adaptive Risk Manager Engine.

4.2.13 Manual Overrides

While computing alerts, actions and score, the Model first consults what has been specified for the manual overrides to see if any of the results need to be overridden.

The manual overrides are a way to specify score, alerts and actions based on specific combination of what is triggered and what isn't triggered for the Rule instance.

You can also use a manual override to trigger another Model based on certain conditions. Example Model "m1" has three Rules m1r1, mar2 and m1r3 and consider the following overrides:

m1r1	m1r2	m1r3	Model/Score		Alert Group	Action Group
True	False	Any	Score	900		
False	False	False	Model	m2	Alert1	

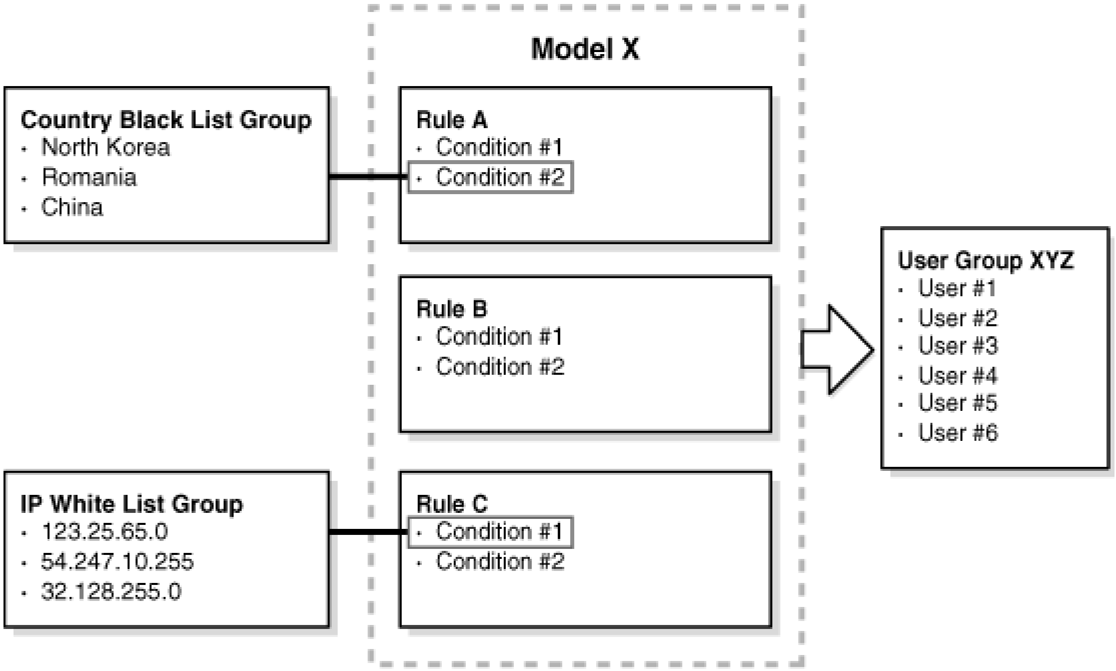
When m1r1 is triggered and m1r2 is not-triggered, a score of 900 is generated and all the alerts and actions generated at Rule instance level become part of the Model result.

When m1r1, m2r2 and m3r3 all Rules are not not-triggered new Model "m2" is called. All Alerts generated at the Rule instance level are ignored and alerts in Alert1 group are generated. All actions from the Rule instances are included in the Model result as action group is not overridden in manual override.

4.2.14 Model

A Model is a container for a collection of related rules and is created based on the policy type. The policy type could be for business, security, or a custom category. A Model is an important building block for a Runtime since Models contain all the information needed to generate the score, list of actions, and alerts.

Models can execute at any time during a user's session.



Model Runtimes include:

- Pre-Authentication Models-Pre-authentication Models contain Rules that are invoked before the user logs in. For example, the user name might not be available at the time that a Rule is invoked. If so, it can't be used to validate whether the user should be allowed to login from the device he/she is using and/or the location from where the user is trying to login.

- Post-Authentication Models-Post authentication Models contain Rules that run after the user enters his/her credentials. These Rules can complement the pre-authentication Rules and are designed to execute after the user attempts to log in.
- In-Session/Transaction Models-Rules from In-Session Models are executed during transactions after the user has completed login successfully. For example, an in-session Rule can be used to reevaluate a user if he/she attempts to transfer funds from one account to another.

Model can be linked to all users or a user group from the Run Mode dropdown of the Model Details page. Run Mode provides "All Users" and "Linked Users" as options. The "All Users" option links a Model to all users.

The default is "Linked Users." If there is a group linking in the model to a specific user group, then the linked users selection will denote that the model will only act upon that user group.

Once a Model is linked to all users or a group of users, the Rules will be used to evaluate user activity.

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

4.2.14.1 Linking Models to Users

Model can be linked to a user group or all users.

Each user belongs to one or more groups. When a user is evaluated for a given Runtime, the Rules Engine builds a Policy Set (set of Models of the same type) based on the user group that the user is associated with and the Model that is linked to the user group.

Examples are provided below.

For the examples, assume that there are four Models--m1, m2, m3 and m4--for the "pre-authentication" Runtime.

Model m1 is linked to the user group, "usergroup1," and model m4 is linked to user groups "user group2" and "user group 3". m2 and m3 are linked to "All users."

All Models belong to same Policy Type.

Case 1

When a user u1 that belongs to user group2 and user group3 is evaluated for the "pre-authentication" Runtime, the Rules Engine builds a Policy set with the following Models and evaluates the Policy Set:

- m2
- m3
- m4

Case2

When a user u2 that belongs to user group1 and user group2 is evaluated for the "pre-authentication" Runtime, the Rules Engine builds a Policy Set with the following Models and evaluates the Policy Set:

- m1
- m2
- m3
- m4

Case3

When a user u2 that belongs to user group4 is evaluated for the "pre-authentication" Runtime, the Rules Engine builds a Policy Set with the following Models and evaluates the Policy Set:

- m2
- m3

4.2.14.2 Advantages of Linking a Model to a User Group

There are two ways to link a Model to users:

- by linking the Model to user groups
- by linking the Model to all users

When should you link a Model to a user group or link the Model to all users?

Linking a Model to all users facilitates evaluation because the Model is evaluated for all users. Group linking allows Model evaluation to be targeted. For example, you can run Model "m" for a certain category of users. Linking Models to a user group is particularly useful when a single Adaptive Risk Manager is used for multiple client applications since Models target each application.

For example, Bank A wants to use Adaptive Risk Manager to prevent fraud for their retail banking and also for their loan approval process. In this example, the client applications are "Loan Approval" and "Retail Banking." Bank A can have some Models for Loan Approval and a different set of Models for "Retail Banking."

4.2.15 Policy Type

Policy Type defines a Model. All Models of the same type are grouped as a Policy. Policy Type is mainly used for scoring purposes.

4.2.16 Policy Set

A Policy Set is for logical grouping of policies used to evaluate traffic in order to identify possible risk and to take action to counter fraud.

4.2.17 Runtime

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

Example Runtimes are:

- View Check Image

- Forgot Password
- Forgot Username
- User Preferences
- Request Secure Document
- Edit Records

4.2.18 Rules Result

The Rules Engine returns a Rules result for each Runtime and contains the final action, list of actions, and score. An example of the final action is "block" / "challenge". An example action list is "block, challenge, background check" and an example score is 800. The typical usage is when the client application acts based on the final action. However, it is possible for the client application to see the other actions that are generated and perform different actions based on those. It is also possible for the client application to create Models a certain way in which the Models generate scores and act on these scores.

5

Auto-learning and Patterns

Auto-learning is a profiling process in which an administrator defines behavior patterns. These patterns are in turn used by Adaptive Risk Manager to dynamically create and populate buckets based on the pattern parameters. Adaptive Risk Manager automatically records/maintains the bucket memberships of the users/devices/locations (entities in general) over time so that the profiles created can be used to evaluate risk.

The Auto-learning feature profiles transactions and authentications being performed by different actors (entities). This process establishes what is normal or average behavior for an individual or a population. In turn this allows evaluations to be made that can determine if a situation is an anomaly and therefore potentially fraudulent. The task is accomplished by

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

This chapter contains the following sections:

- Pattern Creation and Population
- Pattern Evaluation
- Pattern Population
- Pattern Reports

5.1 Pattern Creation and Population

Patterns are either created in single-buckets or multi-buckets where buckets are groupings of behaviors in a broad sense.

5.1.1 Single-Bucket Creation

Single-bucket created patterns have the exact data points, value ranges and/or patterns defined by an administrator. Auto-learning (a set of features that performs adaptive evaluations of risk) can be influenced by creating specific patterns that an administrator wants Adaptive Risk Manager to watch for. Usually these patterns represent behavior considered to be high risk based on industry expertise. An administrator can configure the behavior pattern through Adaptive Risk Manager.

Example

A fraud specialist may configure a pattern so that Adaptive Risk Manager can look for any traffic that falls in the pattern.

A pattern could have the following combination:

- 8am -10am pattern

  and

- New device

  and

- New location

  and

- New transfer account, not owned by this user is created

  and

- Wire transfer to new account

5.1.2 Multi-Bucket Creation

Multi-bucket patterns have more data points than single-bucket created patterns. An administrator selects the data points and samples he wants to base the pattern on, and then during post-processing Adaptive Risk Manager queries the historical data to create the bucket combinations that have occurred in the system. Each bucket will automatically keep from overlapping with each other based on the other buckets already in the system.

Example

An administrator specifies the following data points and sample size for auto-creation.

- Transaction = Bill Pay
- Member Types = user, device, location
- Data Point = Time
- Sample size = 2 hours
- Start Time= 00:00
- Retroactive = Yes

Adaptive Risk Manager would then use post-processing cycles to run queries on all the data in the database to build a maximum of 12 patterns for 2-hour time slots in which bill pay transactions have occurred. After creation, the patterns will be populated with user, device and locations that have fallen within each 2-hour pattern. The memberships and associated statistics will be saved in each user, device, and location profile.

If a web application has three possible transactions that need to be monitored (A, B and C). There are a finite number of patterns that can be created to capture the sequence patterns of these transactions. If transaction data parameter ranges are also being captured, the number of possible patterns increases.

Example

Pattern creation parameters are defined to only capture transaction type. There are three transaction types (A, B and C) in the application so patterns will be created based on these.

5.2 Pattern Evaluation

Risk level is calculated based on the combinations of pattern memberships for the user/device/location being used. The more elements are outside of their normal membership, the higher the risk.

Example 1

Login time will be profiled as part of the pattern risk assessment. For this example, login time patterns will be manually defined. The time patterns are organized around normal business hours in a single time zone. This pattern might be utilized for internal enterprise use for regional offices in that time zone and/or if the local time of the user is known.

Patterns	Time Range
Pattern #1	0:00 to 4:59
Pattern #2	5:00 to 8:59
Pattern #3	9:00 to 16:59
Pattern #4	17:00 to 23:59

After a month of recording, the system finds the following three independent pattern 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	= high risk [device in #4]
If User A logs in at 8:27 using Device X from IP Y	= medium risk [device & IP in #2]
If User A logs in at 11:15 using Device X from IP Y	= very low risk [all in #3]

The first scenario is shown in more granular detail below.

If User A logs in at 3:37 and they have previously only logged in between 9:00 and 16:59 that elevates the risk. If Device X is used and it has previously only been used between 5:00 to 23:59 that elevates the risk. 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 all three of the major components involved in the risk evaluation are not in pattern #1 the overall risk level is very high. It's important to emphasis that each of these elements is evaluated for membership in the time profiles independently in this example.

Example 2

The next example presents a view of the evaluation of pattern membership and the amount of variance by using the same patterns as the previous example but with different memberships and scenarios.

Pattern	Time Range
Pattern #1	0:00 to 4:59
Pattern #2	5:00 to 8:59
Pattern #3	9:00 to 16:59
Pattern #4	17:00 to 23:59

After a month of recording, the system finds these three independent pattern memberships.

Entity	Membership
User A	[#3]
Device X	[#1, #2, #3, #4]
IP Y	[#1, #2, #3]

Evaluation of the memberships and taking variance into account produce 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	= upper medium risk [user is not in #1 or its immediate neighbor #2]
If User A logs in at 8:27 using Device X from IP Y	= lower medium risk [user is not in #2 but they are in its immediate neighbor #3]

5.3 Pattern Population

Patterns are populated and maintained based on the number of successful outcomes. The membership of patterns is constantly reevaluated. The threshold values that govern membership evaluation is independently configurable for each pattern. If he wants, an administrator can apply a configuration to a selection of multiple patterns with a single operation.

Example

Joe regularly logs in from three cities (home, office A and office B). All cities in the Tri-State area including these three had a pattern created for each of them when the system was configured. Joe belongs to the following three city patterns currently.

Pattern	Location
City Pattern #1	[home]
City Pattern #2	[office A]
City Pattern #3	[office B]

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. To become a member of a pattern, an employee must successfully answer the challenge the first two sessions he access the system from that city. To continue membership in pattern #3, Joe must successfully utilize an IP from that city at least once a month. If he stops working at office B for 37 days and does not access from anywhere else in that city, he will be removed from group #3 automatically by Adaptive Risk Manager. If he goes back to office B after his absence he will be challenged for an OTP since he is no longer a member of pattern #3.

5.4 Pattern Reports

Statistical and aggregate queries/templates are provided by Adaptive Risk Manager so that administrators can view pattern membership totals, percentages, and so on. Pattern reports, which are available through BI, provide data based on the pattern information.

- **BucketsByPatternAndMember**: lists all buckets based on pattern and member type for the time range specified.
- **MemberEntitiesByPattern**: lists all metadata for the member entity based on the pattern selected.
- **MembersByPattern**: lists all members based on the pattern selected.
- **PatternsByMember**: lists all patterns available based on the Member Type.
- **PatternsByMemberEntities**: lists all patterns that have the specific metadata as its member entity.

6 Transaction Definitions

A Transaction is any process a user performs after successfully logging in. Examples of Transaction Types are authentication, bill pay, money transfer, merchant purchase, credit card, and others. For example, if you pick merchant purchase as the Transaction Type, you want to gather data on the activity of all the members during merchant purchases.

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

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

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

7 Cases

Oracle Adaptive Access Manager provides a set of tools for creating and supporting two different types of cases: Customer Service Representative (CSR) Cases and Agent Cases.

- *CSR Cases* are used in customer care situations associated within the normal course of doing business online and over the phone when providing assistance to customers. The customer support representatives can use the CSR set of tools for handling inquiries associated with adaptive risk manager.

  A CSR case can be changed to an agent case by CSR managers, investigators and investigation managers.

- *Agent Cases* are used specifically by fraud investigators and investigation managers for analyzing data and finding relationships between sessions and cases. Only investigators and their managers will have access to agent cases.

  An agent case cannot be de-escalated to a CSR case, which is used by customer service representatives and customer service managers.

7.1 CSR Cases

7.1.1 Case Creation

A CSR case is a record of related customer care events and actions for a single customer. Multiple cases also provide a way of segregating unrelated issues and actions for a customer.

CSR cases are used by the customer service representative while assisting a customer.

7.1.2 CSR Case Details

The CSR Case Details page will display the following details for a case.

General Case Details

- Case Created - The date and time the case was created.
- Case Status - The case status can be New, Pending, or Closed. When a case is created, the status is set to New by default.
- Severity Level - The severity level is set by whomever creates the case and used as a marker to communicate to users how severe this case is.
- Case Type - Agent or CSR

- Disposition - When a case is closed the disposition describes the way in which the issue was resolved. Cases only have dispositions when they're closed. If a case has any status besides closed, the disposition is blank.
- Expiration Date: Date when CSR case expires. By default, the length of time before a case expires is 24 hours. After 24 hours, the status will change from New to Expired. After the case expires, the CSR user will not be able to open the case anymore, but the CSR manager will be able to. The length of time before a case expires is configurable in the customercare.properties file. Refer to the *Oracle Adaptive Access Manager Developer's Guide* for details for configuring the expiry behavior.
- Description - The details for the case. A description is required.
- Last Case Action - The last action executed for this user in the CSR case
- Date of Last Case Action - The date when last action occurred.
- Last Global Case Action - The last action that occurred for this user (identified by a combination of the Username and User ID) in ALL CSR cases. Agent cases are not taken into account.
- Date of Last Global Case Action - The last action perform against the user online.

User Data

- Username - User for whom case is created
- User ID - Encrypted username
- Application ID - The ID of the application.
- Last Online Action - The last action that user executed, for example - Answered challenge question would show "Challenge Question" or if user is blocked, "Block."
- Date of Last Online Action - Date when last online action was executed.
- Temporary Allow Expire Date - When temp allow is enabled; this field tells you when it expires. If temporary allow is 7 days, the expiry date will be a week from today.
- Temporary Allow Active - If temporary allow is active, this field shows "Yes;" otherwise the field shows "No."
- Completed Registration - If user has completed registration, this field shows "Yes;" otherwise it shows "No." The user must complete all of the following tasks: personalizing a textpad (image and phrase), and registering security questions and answers.
- Questions Active - If user has completed registration, but questions have been reset, and he hasn't gone back and registered new ones, this field would display "No." This field shows "yes" if the user has completed registration and questions exists by which he can be challenged.
- Personalization Active - When user has an image, a phrase and questions active, this field would display "Yes." If any one of these are reset, this field would display "No."

7.1.3 Device Registration Actions

Your customers can elect to register their device during registration. A customer might, for example, register his office or home computers, but not register a computer he might use on a business trip.

The rules administrator could then write or configure rules based on a device registered flag. For example, he could configure a rule that would always challenge the customer if his current device is not registered. Or, he could create a larger rule that would take the fact that the device is not registered into account.

As a CSR, you can unregister all of a customer's devices through the Actions tab on the Case Details page.

7.2 Agent Cases

7.2.1 Case Creation

Agent cases are tools for investigators and investigation managers to facilitate an investigation by identifying the data and relationships. By linking sessions and cases, Oracle Adaptive Access Manager can locate relationships between sessions in which an suspicious activity has occurred or sessions in which alerts were generated.

For Agent cases, any number of sessions can be selected for linking to the new case. These sessions are the basis for the new case relationships.

7.2.2 Agent Case Details

Agent cases will display general case details.

General Case Details

- Case Created - The date and time the case was created.
- Case Status - The case status can be New, Pending, or Closed. When a case is created, the status is set to New by default.
- Severity Level - The severity level is set by whomever creates the case and used as a marker to communicate to users how severe this case is.
- Case Type - Agent or CSR
- Disposition - When a case is closed the disposition describes what the resolution was. If a case has any status besides closed the disposition is blank.
- Expiration Date - Date when agent case expires
- Overdue - If a case is open and has not been accessed longer than the time range set the overdue flag will be set to allow managers to see cases needing attention. For example, if Agent cases are set to 24 hours then the flag will be set to "overdue" if a case is open and has not been accessed in more than 24 hours. An overdue case will be refreshed for another 24 hours if an investigator accesses it. The overdue behavior is configurable in the customercare.properties file. Refer to the *Oracle Adaptive Access Manager Developer's Guide* for details.
- Description - description of the case.
- Last Case Action - The last case action executed for this Agent Case. There are no user details in agent cases.

- Date of Last Case Action - Date when last case action was executed.

7.2.3 Linked Sessions and Data

Sessions and/or data that an investigator feels have specific importance to a case may be linked to a case.

Linked sessions are displayed in a listing. A column exists for each entity from each session. In addition, a column exists for each Runtime, displaying any triggered alerts from that Runtime. This allows for sessions containing different data types to be linked.

Runtimes are displayed with the execution time and transactions, and their attributes are displayed with the transaction ID. When a session is linked to a case, notes are required to explain the reason. In addition, an importance level is set when the link is created. This importance level is a filter for investigation.

Data is linked to a case automatically when the case is created. Linked data is used to generate the related sessions and cases, which are displayed in the related area. Each data type and individual piece of data can be selected/de-selected to be used in the calculation of related cases and sessions. The current state of the case screen is preserved if a user leaves and then returns. This includes all display settings and states.

Example

An investigator could identify three sessions which were found to contain similar fraud. The sessions could be selected from a query and linked to an existing case or a new case can be created using these linked sessions. The entities (user, device, location, credit card, ship address, etc.), Runtimes and alerts from the three sessions would be used to determine what sessions and cases are related to the case. If sessions are added or removed from the list of linked data the related list will be altered.

Example

If a case is created automatically by an action, the linked data will be taken from the session in which the action was triggered. The case will contain all the major data points from that session such as entities, Runtimes and alerts.

Example

If a case is created from the Search User Cases screen, the linked data will contain data from sessions selected in the provided search screen based on user.

Example

If the data type "IP address" is de-selected in the user interface, no related cases or sessions will be displayed based on the IP address used.

Example

If two specific devices are deselected in the linked tab then those two data points will not influence the related sessions shown.

7.2.4 Overdue (Agent Case Default)

Only an administrator can configure the overdue duration. If a case is open and has not been accessed longer than the time range set, the overdue status is set to allow managers to view cases needing attention. A report template is provided that displays all overdue cases. The report runs on a regular schedule (daily by default). The report is sent via email to the investigation managers.

Example

If agent cases are set to 24 hours, the status will be set to "overdue" if a case is open and has not been accessed in more than 24 hours. An overdue case will be refreshed for another 24 hours if an investigator accesses it.

Example

If a CSR case is escalated to an agent case, it starts the overdue timer from that point forward.

7.2.5 Related Sessions and Cases

7.2.5.1 Related Cases

Cases that share data with the linked sessions are related and are displayed in Related Cases. Search parameters are available to further narrow the view. The cases will display the data points by which they are related. Each case number will contains links to the case.

Example

If the user ID "jsmith" is in the linked sessions data, all cases involving jsmith in its links will be shown in the related listing.

7.2.5.2 Related Sessions

Sessions that share data with the linked sessions are related and will be displayed in Related Sessions. Search parameters are provided in Filter Related Sessions/Cases to further narrow the view.

Example

If the user ID "jsmith" is in the linked sessions data, all sessions involving jsmith will be shown in the related listing.

8

Device Registration

Device registration is a feature that allows a user to flag the computer he is using as a safe device. The customer can then configure the rules to challenge a user that is not coming from one of his registered devices.

Device registration is available as a standard feature in Oracle Adaptive Access Manager. The feature can be turned on, although it is off by default in the product.

8.1 Enabling Registration

Adaptive Strong Authenticator and Sample (an application that is packaged with Oracle Adaptive Access Manager as an example for customers) have a property driven feature that allows device registration for users. When the property is set to true, configurable messaging and a checkbox appears on the challenge screen under the QuizPad. For information on enabling the device registration feature, refer to the *Oracle Adaptive Access Manager Developer's Guide*.

The device registration text and checkbox is only shown during the login flow challenge. By default the checkbox will be checked; however, this default state will be configurable via properties. When the checkbox is checked, the device is added to the user's profile as a registered device. If a device is already registered, the checkbox and messaging is not displayed on the screen.

If a user chooses not to register a device (un-checks the box) and then logs in successfully, the next time he logs in with that device, the box will be unchecked. The User Preferences page will contain actions to unregister the current device and one to unregister all his devices.

8.2 Checking Registration

A rule to check for registration is available in Oracle Adaptive Access Manager. This rule triggers if the device has been registered in the past by the current user. Also, a rule is available to check if a device has been used before by this user and is not registered. A model containing these rules is available as part of the base models package. This model will be disabled by default so users can enable it only if they want to use device registration.

8.3 Resetting Registration

An action to unregister all devices for a user is available in CSR type cases. This action is called "Unregister Devices." It is a "User item" under the "Customer Resets" action. Unregister Devices will delete all registered devices from the user's profile.

Glossary

Access Authentication

In the context of an HTTP transaction, the basic access authentication is a method designed to allow a web browser, or other client program, to provide credentials – in the form of a user name and password – when making a request.

Action

An event activated when a rule is triggered. For example: block access, challenge question, ask for PIN, and so on.

Agent Cases

Agent Cases are used specifically by fraud investigators and investigation managers for analyzing data and finding relationships between sessions and cases. When an investigator links sessions and cases, Oracle Adaptive Access Manager can search the data for suspicious activity.

Alert

A message generated when a rule is triggered. For example: login attempt from a new country for this user.

Application ID

The primary ID for the user. For example, a user can be part of "bharosauiogrp" and "testgrp, but his Application Id or primary ID will be "bharosauiogrp." Application ID is similar to a userid group.

Attribute

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

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

Authentication

The process of verifying a person's, device's, application's identity. Authentication deals with the question "Who is trying to access my services?"

Authorization

Authorization regards the question "Who can access what resources offered by which components?"

Auto-learning

Auto learning is a feature that analyzes the behavior of user data coming into the system and profiles (creates digest) of the user's data. This data is then stored in a historical data table and used for calculating the risk based on rules. The best advantage of Auto-learning is that the system learns the changes in user's behavior and slowly adapts to it when calculating risk.

Blocked

If a user is "Blocked," it is because a Model has found certain conditions to be "true" and is set up to respond to these conditions with a "Block Action." If those conditions change, the user may no longer be "Blocked." The "Blocked" status is not necessarily permanent and therefore may or may not require an administrator action to resolve. For example, if the user was blocked because he was logging in from a blocked country, but he is no longer in that country, he may no longer be "Blocked."

Bots

Software applications that run automated or orchestrated tasks on compromised PCs over the internet. An organization of bots is known as a bot net or zombie network.

Buckets

Buckets are groupings of behaviors.

Auto-learning patterns are used to dynamically create and populate profiling buckets to track behavior and transactions.

Buckets help in creating the statistics for the entities based on their memberships to various patterns and hour/day/month/year time samples.

Case Created

The date and time the case was created.

Case Description

The details for the case. A description is required for cases.

Case Number

A unique identification number allocated to each case.

Case Status

Case Status is the current state of a case. Status values used for the case are New, Pending, Escalated, or Closed. When a case is created, the status is set to New by default.

Case Type

Type of case.

- CSR - CSR cases are used in customer care situations associated within the normal course of doing business online and over the phone when providing assistance to customers. A CSR case is attached to a user.
- Agent - Agent cases that fraud investigators and investigation managers work on. They are used specifically by fraud investigators and investigation managers for analyzing data and finding relationships between sessions and cases. An Agent case is not attached to any user like a CSR case.

Cases

Case tools for servicing customer needs. Tools enables the institution to review servicing logs for each individual client to investigate the reasons that actions were taken or alerts were triggered.

Challenge Questions

Challenge Questions are a finite list of questions used for secondary authentication.

Configurable Actions

Configurable Actions allow a user to create new supplementary actions that occur after the running of rules.

Completed Registration

Status of the user that has completed registration. To be registered a user may need to complete all of the following tasks: Personalization (image and phrase), registering KBA questions/answers and email/cellphone.

Cookie

A cookie (also browser cookie, computer cookie, tracking cookie, web cookie, internet cookie, and HTTP cookie) is a small string of text stored on a user's computer by a web browser. A cookie consists of one or more name-value pairs containing bits of information such as user preferences, shopping cart contents, the identifier for a server-based session, or other data used by websites. It is sent as an HTTP header by a web server to a web client (usually a browser) and then sent back unchanged by client each time it accesses that server. A cookie can be used for authenticating, session tracking (state maintenance), and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts.

Creation Method (Buckets)

- Single Bucket - Single-bucket patterns will create and populate one bucket with the exact data points and value ranges specified in the pattern
- Multi- Bucket – Multi-bucket patterns have buckets for sub-ranges of a parameter range

CSR

Customer service representatives resolve low risk customer issues originating from customer calls. CSRs has limited access to Adaptive Risk Manager

- View the reason why a login or transaction was blocked
- View a severity flag with alert status to assist inescalation
- Complete actions such as issuing temporary allow for a customer

CSR Cases

CSR Cases are used in customer care situations associated within the normal course of doing business online and over the phone when providing assistance to customers. The customer support representatives can use the CSR set of tools for handling inquiries associated with Adaptive Risk Manager.

CSR Manager

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

Date of Last Case Action

In cases, the date when last action occurred.

Date of Last Global Case Action

The last action performed against the user online.

Date of Last Online Action

Date when last online action was executed

Device

A computer, PDA, cell phone, kiosk, etc used by a user

Device Fingerprinting

A mechanism to recognize the device a customer typically uses to login – whether it is a desktop computer, laptop computer, PDA, cell phone, kiosk, or other web enabled device. The fingerprinting process produces a fingerprint that is unique to the user and designed to protect against the "replay attacks" and the "cookie based registration bypass" process.

Disposition

The disposition describes the way in which the issue was resolved in a case. Cases only have dispositions when they're closed. If a case has any status besides closed, the disposition is left blank.

Device Registration

Device registration is a feature that allows a user to flag the device (computer, mobile, PDA, and others) he is using as a safe device. The customer can then configure the rules to challenge a user that is not coming from one of his registered devices.

Entities Editor

A tool to edit entities, a user-defined structure that can be re-used across different transactions. Only appropriate and related fields should be grouped into an Entity.

Entity

1. A referencible data structure that can be used in transaction definitions or directly in patterns. Entities or actors are users, devices, IP.

2. Entity can be defined as an organized array of individual elements and parts forming and working as a unit

3. Entity is a set of fields. It is like a user-defined structure that can be re-used across different transactions

Expiration Date

Date when CSR case expires. By default, the length of time before a case expires is 24 hours. After 24 hours, the status will change from New to Expired. After the case expires, the CSR user will not be able to open the case anymore, but the CSR Manager will be able to. The length of time before a case expires is configurable.

Evaluation Priority

The priority in which data is evaluated.

- First

  The data is evaluated in realtime (highest priority)

- Second

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

Fraud Investigator

A Fraud Investigator primarily looks into suspicious situations either escalated from customer service or directly from Adaptive Risk Manager alerts. Agents have access to all of the customer care functionality as well as read only rights to security administration and BI Publisher reporting.

Fraud Investigation Manager

A Fraud Investigation Manager has all of the access and duties of an investigator plus the responsibility to manage all cases. A manager must routinely search for overdue cases to make sure none are forgotten.

Fraud Scenario

A fraud scenario is a potential or actual deceptive situation involving malicious activity directed at a company's online application.

Gated Security

The multiple security checkpoints a user must pass through to gain access to sensitive data or transactions.

Groups

Groups allow you to view and administister a collection of like items as a single group. You should assign each group a unique name. The types of groups you can create include User ID, Login ID, Location, Device, Action, and Alert.

HTTP

Hypertext Transfer Protocol

IP address

Internet Protocol (IP) address

KBA Phone Challenge

When a customer's challenge questions are used for phone authentication. If the customer answers the question correctly, the system automatically takes appropriate action depending on their status such as unlocking the customer if they were locked out. If the customer answered the question incorrectly, they will get additional attempts at that question (depending on configuration). If the customer exceeds the maximum number of failures for a question another question will be asked. If two or more questions are asked in this process, and they answer successfully, their questions are automatically reset. If all of the questions were asked and the customer failed all attempts at each question, the customer will be locked out of online access.

KBA (Knowledge Based Authentication)

KBA is a secondary authentication infrastructure for pre-registered challenge questions, the creation, edit, validations, registration, presentation, and answers of challenge questions.

KeyPad

Virtual keyboard for entry of passwords, credit card number, and on. The KeyPad protects against Trojan or keylogging.

Keystroke Loggers

Software that captures a user's keystrokes. Keylogging software can be used to gather sensitive data entered on a user's computer.

Last Case Action

The last action executed in the CSR or Agent case.

Last Global Case Action

The last action that occurred for this user in all CSR cases. Agent cases and Escalated cases are not taken into account.

Last Online Action

The last action that user executed, for example - Answered challenge question would show "Challenge Question" or if user is blocked, "Block."

Location

A city, state, country, IP, network ID, etc from which transaction requests originate.

Locked

"Locked" is the status that Oracle Adaptive Access Manager sets if the user fails a question challenge. The "Locked" status is only used if the One-Time-Password (OTP) facility is in use. OTP sends a one-time password to the user via e-mail or SMS text message. If the user exceeds the number of retries when attempting to put in his OTP code, then his account becomes "Locked." After that, a Customer Service Representative must reset the status to "Unlocked" before the account can be used to enter the system.

Malware

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Malware may contain key loggers or other types of malicious code.

Man-In-The-Middle-Attack (Proxy Attacks)

An attack in which a fraudster is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised

Manual Override

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

Member

The member is the actor for which data needs to be captured.

Model

A Model is a set of rules that run at a single time. A Model contains rules that when linked to a group, are used to evaluate group members. The rules are added to the Model, configured, and linked to groups by the administrator. A new rule can be added to an existing Model at any time. In a Model, you can control the timing and combinations of rule firing with manual overrides.

Mutual Authentication

Mutual authentication or two-way authentication (sometimes written as 2WAY authentication) refers to two parties authenticating each other suitably. In technology terms, it refers to a client or user authenticating himself to a server and that server authenticating itself to the user in such a way that both parties are assured of the others' identity.

Nested Models

A Nested Model is a secondary model used to further quantify the risk score in instances where the original result output by the system is inconclusive. Nested Models can be assigned to ensure a higher degree of accuracy for the risk score. A Nested Model is run only when a specific sequence of answers is returned from the primary Model. Nested Models therefore reduce false positives and negatives.

One-Time PIN/Password

Generation and delivery of a single use volatile credential. For example: Server generated, hand-held device, software generated, and so on. The purpose of a one-time pin/password (OTP) is to make it more difficult to gain unauthorized access to restricted resources, like a bank account. Traditionally static passwords can more easily be accessed by an unauthorized intruder given enough attempts and time. By constantly altering the pin/password, as is done with a one-time pin/password, this risk can be greatly reduced.

Oracle Adaptive Access Manager

A product to protect the enterprise and its customers online.

Out Of Band Authentication

The use of two separate networks working simultaneously to authenticate a user. For example: email, SMS, phone, and so on.

Overdue

A flag that will signal when a case has not been accessed in a given time range. The overdue flag is set to allow managers to see cases that require attention.

Patterns

A composite of traits or features characteristic of an individual or a group. One's pattern of behavior.

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

- An individual's location is from USA and from his home desktop
- The accounts group processes orders between 8AM-1PM
- A user transfers amount between 100$ to 200$ once a week to his overseas account

Personalization Active

Status of the user who has an image, a phrase and questions active. Personalization consists of a personal background image and phrase. The timestamp is generated by the server and embedded in the single-use image to prevent reuse. Each Authenticator interface is a single image served up to the end user for a single use.

Pharming

Pharming (pronounced farming) is an attack aiming to redirect a Web site's traffic to another, bogus Web site.

Phishing

A criminal activity utilizing social engineering techniques to trick users into visiting their counterfeit Web application. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity. Often a phishing exercise starts with an email aimed to lure in gullible users.

PinPad

Authentication entry device used to enter a numeric PIN.

Plug-in

A plug-in consists of a computer program that interacts with a host application (a web browser or an email client, for example) to provide a certain, usually very specific, function "on demand".

Policy Set

A policy set is the collection of all the currently configured policies used to evaluate traffic to identify possible risks. As a failsafe, an action override or a score override can be created for a policy set so that the override is automatically invoked to override a particular action triggered by a rule when a specific set of circumstance occurs.

Policy Type

The Policy Types are Security and Business.

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

Risk Score

The numeric risk level associated with a Runtime.

Questions Active

Status of the user who has completed registration and questions exists by which he can be challenged.

QuestionPad

Device that presents challenge questions for users to answer before they can perform sensitive tasks. This method of data entry helps to defend against session hijacking.

Rule Conditions

Rule conditions are the building blocks and make the rule-related functions in Oracle Adaptive Access Manager available to the client.

Rules

Rules are housed in Models, identify and react to certain information, and trigger actions, alerts, and scores. Rules can be added to Models, and Models can be applied to a group of users or all users.

Runtime

A Runtime is a specified point in a session when rules in a model will run. For example, at pre-authentication, post-authentication, and in-session. Risk can be evaluated at any time specified by a Runtime. To gain access to sensitive data or transactions a user must successfully pass through multiple security checkpoints.

Scores & Weights

Score refers to the numeric scoring used to evaluate the risk level associated with a specific situation. Weight refers to the multiplier used to influence the total score at various evaluation levels. Weight is only applied to a score when a given Model or Policy type is using a "weighted" scoring engine.

Scoring Engine

Fraud analytics engine you want to use to calculate the numeric score that determines the risk level. The various engines are listed below along with examples of how each scoring engine would calculate a Model Score.

- Aggregate Score

  Sum of the scores of all fired Rules.

- Average

  Average = (sum of scores of all fired Rules) / (count of all Rules used)

- Maximum

  Higher score out of all fired Rules

- Minimum

  Lower score out of all fired Rules

- Weighted Average

  [Average =(sum of scores of all fired Rules) / (count of all Rules used)] * (weight modifier specified by Model)

- Weighted Maximum Score

  (larger score out of all fired Rules) * (weight modifier specified by Model)

- Weighted Minimum Score

  (lower score out of all fired Rules) * (weight modifier specified by Model)

Restricted Note

A note describing why an action was taken in a case. A "Restricted" note can only be written by investigators and read by customer service managers and investigators.

Security Token

Security tokens (or sometimes a hardware token, hard token, authentication token, USB token, cryptographic token) are used to prove one's identity electronically (as in the case of a customer trying to access their bank account). The token is used in addition to or in place of a password to prove that the customer is who they claim to be. The token acts like an electronic key to access something.

Severity Level

A marker to communicate to case personnel how severe this case is. The severity level is set by whomever creates the case. The available severity levels are High, Medium, and Low. If a customer suspects fraud, then the severity level assigned is "High." If the customer wants a different image, then the severity level assigned is "Low." Severity levels of a case can be escalated or de-escalated as necessary.

Session Hijacking

The term Session Hijacking refers to the exploitation of a valid computer session - sometimes also called a session key - to gain unauthorized access to information or services in a computer system

SOAP

SOAP, originally defined as Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on Extensible Markup Language (XML) as its message format, and usually relies on other Application Layer protocols (most notably Remote Procedure Call (RPC) and HTTP) for message negotiation and transmission. SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built.

Social Engineering

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information to a fraudulent entity.

Spoofing Attack

In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Spyware

Spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.

Standard Note

A note describing why an action was taken in a case. A "Standard" note can be written and read by customer service representatives, managers, and investigators.

Status (Pattern)

Status is the current state of a Pattern.

- Active - If data needs to be collected, the pattern must be in the active state.
- Inactive - If the pattern is complete, but you don't want to collect data, pick "Inactive."
- Incomplete - If pattern creation has started, but you need to save it for completion later, choose "Incomplete." Data is not collected for this state.
- Invalid - The administrator may choose to mark the pattern as invalid if he does not want the pattern used. Data is not collected for this state.

Strong Authentication

An authentication factor is a piece of information and process used to authenticate or verify the identity of a person or other entity requesting access under security constraints. Two-factor authentication (T-FA) is a system wherein two different factors are used in conjunction to authenticate. Using two factors as opposed to one factor generally delivers a higher level of authentication assurance.

Using more than one factor is sometimes called strong authentication.

Temporary Allow

Temporary account access that is granted to a customer who is being blocked from logging in or performing a transaction.

Temporary Allow Active

Temporary allow is active.

Temporary Allow Expiration Date

Date when temp allow expires.

TextPad

Personalized device for entering a password or PIN using a regular keyboard. This method of data entry helps to defend against phishing.

Transaction Definition

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

Trojan/Trojan Horse

A program that installs malicious software while under the guise of doing something else.

User

A business, person, credit card, etc that is authorized to conduct transactions.

Virus

A computer program that can copy itself and infect multiple computers without permission or knowledge of the users.

Index