Adaptive Risk Manager Offline

PoC Guide

10*g* (10.1.4.3.0)

December 2007

Adaptive Risk Manager Offline PoC Guide, 10g (10.1.4.3.0)

Contents

PoC

Objectives

- Ensure that proposed Adaptive Risk Manager Offline solutions meet client's objectives for fraud management and detection.
- Conduct simulation with real customer data with Adaptive Risk Manager Offline tool.
- Compare Adaptive Risk Manager Offline alerts with client "truth set".
- Provide best practices, business, and technical knowledge of Adaptive Risk Manager Offline and solutions to client.

Implementation Details

- Optionally, during the PoC, Oracle will work with client's tech resources to install the Adaptive Risk Manager Offline into client's environment.
- Oracle will populate the data—either from an internal DB (client source) or from an XML file provided by the client—into Adaptive Risk Manager Offline.
- The security rules will be run against this data and alerts will be generated for suspicious activities.
- These suspicious activities will then be compared against the client's truth set(s).

Results

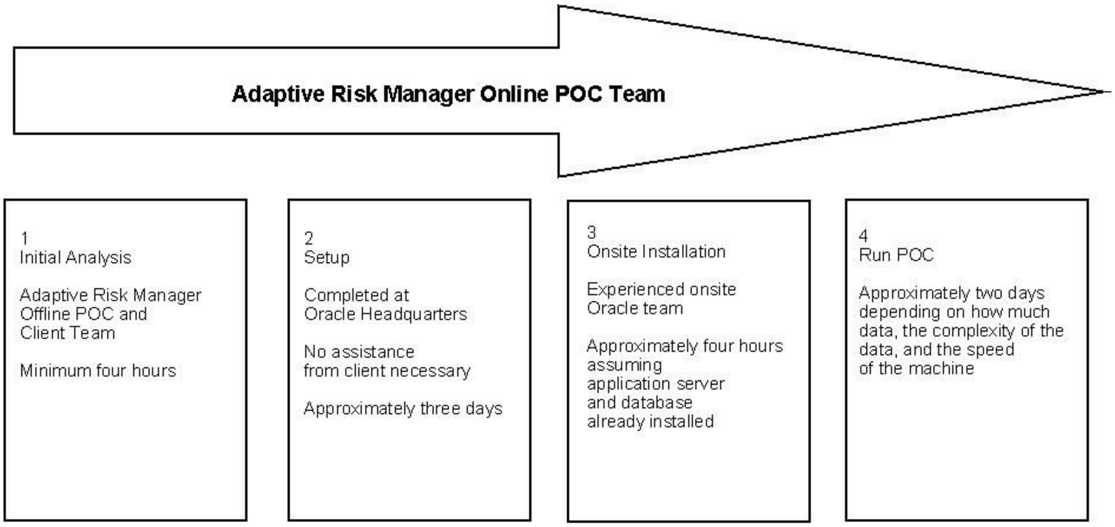
- Results include:
  - Potential fraudulent activities
  - Alerts triggered, alert type, and alert level.
  - Auto generated suspicious fraud cases
  - Models and rules triggered
  - Customer activity by geographical boundaries
  - Devices used
  - Transactions
  - The progress of the risk analysis data can be monitored using the dashboard.
- Adaptive Risk Manager Offline's PoC team will work with the institution's business and/or fraud teams for detailed comparative analysis against truth set(s).

Advantages

Adaptive Risk Manager Offline’s PoC will:

- Help you understand your customers better.
- Highlight weaknesses in the existing customer's transaction system.
- Provide trends in various types of fraudulent activities.

Recommended Timeline



Adaptive Risk Manager Online POC Team

1
Initial Analysis

Adaptive Risk Manager
Offline POC and
Client Team

Minimum four hours

2
Setup

Completed at
Oracle Headquarters

No assistance
from client necessary

Approximately three days

3
Onsite Installation

Experienced onsite
Oracle team

Approximately four hours
assuming
application server
and database
already installed

4
Run POC

Approximately two days
depending on how much
data, the complexity of the
data, and the speed
of the machine

Integration Timeline

Adaptive Risk Manager Offline Integration	**Work**	**Duration**	**Start**	**Finish**	**Predecessors**
Objective					
Team-to-Team Meeting					
Kickoff Meeting					
Deliverables					
Product Charter					
Project Plan					
Milestone 1: Project Governance Complete					
Define					
Consolidated Requirements Document					
Use Case Document					
Acceptance Criteria Document					
Milestone 2: Definition Documents Complete					
Design					
Integration Documents					
Architecture Diagram					
Network Diagram					
Page Flow Diagram					
Design Review					
Milestone 3: Design Documents Complete					
Develop Reference Implementation					
ARM Offline Installation					
Reference Development					
Configuration and Customization					
Functional Acceptance Test					

Adaptive Risk Manager Offline Integration	Work	Duration	Start	Finish	Predecessors
Package Reference Implementation					
Milestone 4: RI Functional per Spec					
Deliverables					
Server Installation Package					
Client Installation Package (.NET)					
ARM Offline integration document					
Database setup document for ARM offline					
ARM Offline Administrator's Guide					
Deploy Reference Implementation (Dev)					
ARM offline Installation					
RI Demonstration/Code Walkthrough					
Capacity Planning					
Functional Acceptance Test					
Configuration Revisions					
Milestone 5: RI Functional at Client					
Deploy QA					
Developer Support					
Configuration Revisions					
Integration Development/Testing					
Design/Code Review					
Milestone 6: Deployed in QA					
Deploy Production					
Functional Production					
Functional Testing					
Regression Testing					
Vulnerability Testing					
Performance Testing					

Adaptive Risk Manager Offline Integration	Work	Duration	Start	Finish	Predecessors
Production Deployment					
Training					
Client Communication					
Milestone 7: Deployed in Production					

Adaptive Risk Manager Offline

Overview

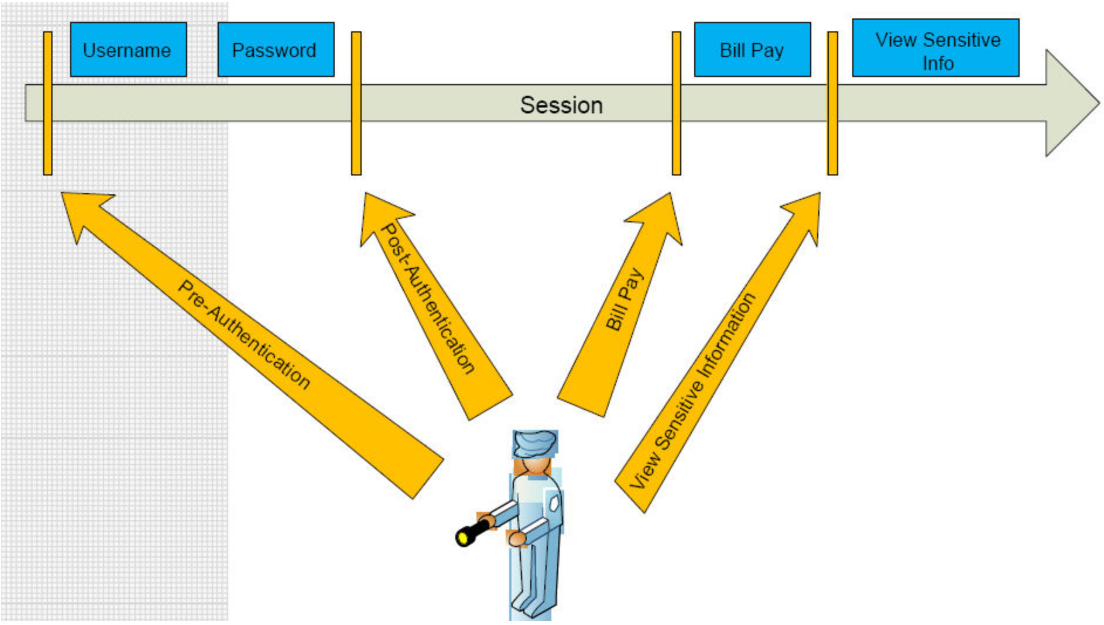
Adaptive Risk Manager Offline is an offline fraud analysis tool that evaluates existing transaction data for two main purposes:

- 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 real-time environment.
- Adaptive Risk Manager Offline is an offline configuration and investigation tool for analysis and development of risk mitigation strategies.
- Adaptive Risk Manager Offline enables you to pre-visualize the effectiveness of models and rules.
- Historical data can be loaded from a real-time Adaptive Risk Manager Database or from the institution's own data source(s).

Runtimes and Models

Runtimes

Adaptive Risk Manager Offline can run its pre-defined models in different runtimes depending on the data received from the client.



Rules Engine

Login Runtime and Model

Login models include the following rules:

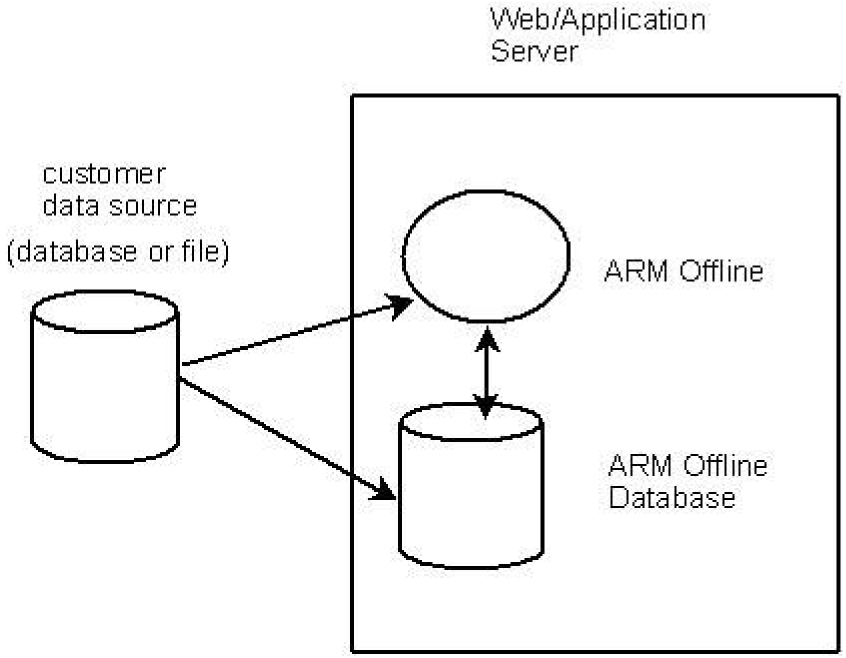
- Device identification rules
  - Suspicious user agent string
  - Max number of devices per user
- Location rules
  - Restricted countries
  - Suspicious IP routing type, IP address, carriers
  - Max number of countries/states per user within timeframe
- Velocity rules
  - Max number of login attempts per timeframe for given device
  - Max users per timeframe for given device
  - Max number of invalid attempts by user within timeframe
- Non plausible rules
  - Non plausible location – i.e. user signs in from NY, then from CA within 10 minutes
- User behavior/Anomaly rules
  - Login time differs from previous login times
  - User agent string is different from previous user agent string of same device
  - IP routing type differs from previous logins

Transaction Runtime and Model

Transaction models include rules such as:

- Suspicious stock transaction – i.e. stock manipulation, “pump & dump” schemes
- Max number of payments to same payee within timeframe
- Max number of high dollar amount transactions within timeframe
- First time device/location and adding new payee
- Max number of accounts opened from same device/location within timeframe
- New account opening with immediate money transfer capabilities from first time device/location

Deployment Architecture



Prerequisites and Dependencies

The prerequisites and dependencies for the installation and configuration of Adaptive Risk Manager Offline are summarized in the table below.

Prerequisites and Dependencies	**Descriptions**
Java	Java Runtime Environment, version 1.5 or higher, needs to be installed. Environment variables JAVA_HOME and PATH must be set appropriately.
Adaptive Risk Manager Offline database	Adaptive Risk Manager Offline has its own database that has an identical schema to that of the Adaptive Risk Manager Online version. Customer login and/or transaction data must be loaded into the Adaptive Risk Manager Offline database, and Adaptive Risk Manager Offline uses this database to perform risk analysis. For the Adaptive Risk Manager Offline database, follow the instructions in the *Oracle Adaptive Access Manager Database Installation Guide for Oracle* or the *Oracle Adaptive Access Manager Database Installation Guide for SQL Server* for creating the database schema and populating it with the default values.
File Write Permission	The Adaptive Risk Manager Offline Server writes activity logs to rolling log files. The verbosity of the logs can optionally be configured using standard log4j.xml configuration.
Port Configuration	Ensure that the port used by the Adaptive Risk Manager Offline Application server is accessible to the client machine. You are allowed to configure the port number.

System Requirements

RAM

1.5 GB Minimum

Database

- Oracle 9i or later
- MySQL 2005

Application Server

- Oracle Application Server
- WebLogic
- WebSphere
- Tomcat
- Pramati
- MSSQL server

Software

- JDK 1.5 or later
- JDBC driver

Operating System

- Redhat Linux
- Windows XP or later
- Solaris
- HP-UX
- AIX

Performance

Note: You must restart the machine in order for some of the settings to take effect.

JVM Settings

The Minimum Memory setting is 1024 MB.

For high volume deployments, please perform load testing to come up with ideal settings.

Installation Details

Database Installation

For the Adaptive Risk Manager Offline database, follow the instructions in the *Oracle Adaptive Access Manager Database Installation Guide for Oracle* or the *Oracle Adaptive Access Manager Database Installation Guide for SQL Server* for creating the database schema and populating it with the default values.

IP Location Data

For information on importing the IP location data into the Adaptive Risk Manager Offline database, refer to the *Oracle® Adaptive Access Manager IP Location Data Import Guide*.

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

Note: The process of loading the information may take around 5 hours.

Deploying Adaptive Risk Manager Offline

Refer to the *Adaptive Risk Manager Offline Installation Guide* for the requirements and instructions for its deployment in WebLogic, Tomcat, WebSphere, and Oracle 10g Application Server.

Configuring TopLink

Refer to the *Adaptive Risk Manager Offline Installation Guide* for instructions.

Configuring Server Properties

Refer to the *Adaptive Risk Manager Offline Installation Guide* for instructions.

Usage

Refer to the *Adaptive Risk Manager Offline Administrator's Guide* for instructions on

- The Standard Loading Process
- Creating a Load Configuration
- Defining a Session Set
- Starting the Load Process
- Risk Analysis

Customized Loading Process

Please refer to the *Adaptive Risk Manager Offline Customized Loader Framework* manual.