Oracle® Adaptive Access Manager

Installation and Configuration Guide

Release 10*g* (10.1.4.5)

E12050-03

May 2009

ORACLE®

Oracle Adaptive Access Manager Installation and Configuration Guide, Release 10*g* (10.1.4.5)

E12050-03

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

15 Configuring Client Properties

16 Setting Up Logging

17 Globalization Support

18 BI Publisher Reports

19 Multi-Tenant Support

20 What to Do Next

C Upgrading from 3.5 to 10.1.4.3

D Encryption Reference

E Archive and Purge

Preface

The *Oracle Adaptive Access Manager Installation and Configuration Guide* provides information about basic installation and setup of Oracle Adaptive Access Manager components.

Audience

This guide is intended for administrators who are responsible for installing and configuring any Oracle Adaptive Access Manager component.

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 Concepts*

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.

1

Installation and Configuration Overview

This chapter provides an introduction to the architecture, installing and configuring of Oracle Adaptive Access Manager. Topics include

1.1 Oracle Adaptive Access Manager

Oracle Adaptive Access Manager (OAAM) is Oracle Identity Management's solution for web access real-time fraud detection and multi-factor online authentication security for the enterprise. Oracle Adaptive Access Manager includes two core components.

Adaptive Risk Manager Web Application (ARM)

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.

Adaptive Risk Manager comes with:

- Rules Engine embedded
- SOAP Server
- Admin Console
- Fraud Case Management tool
- Fraud Investigation tool

Adaptive Strong Authenticator Web Application (ASA)

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.

Adaptive Strong Authenticator comes with:

- Rules Engine embedded (optional)
- Best practice security user flows
- Out of the box models for managing registration flows
- Support for upgrading security preferences
- Common base for Universal Installation Option, Access Management, SAML integrations

1.2 Oracle Adaptive Access Manager Integrations

All the integration options are listed below. This section contains the following topics:

- Native Integration
- Universal Installation Option Integration
- Access Management Integration
- SAML Integration

1.2.1 Native Integration

The client portion of Oracle Adaptive Access Manager can be natively integrated. In the native integration, the client application invokes the Oracle Adaptive Access Manager APIs directly and manages the authentication and challenge flows. The Adaptive Strong Authenticator web application is not used in this integration.

SOAP/Web Services and Static Linked Integrations

The two flavors of native integration are:

- SOAP/Web Services Integration

  The web application communicates with Adaptive Risk Manager Online using the Adaptive Risk Manager Online Native Client API or via Web Services.

- Static Linked (In Proc) Integration

  The native integration involves only local API calls and therefore no remote server risk engine calls. The integration embeds the processing engine for Adaptive Risk Manager with the application and enables it to leverage the underlying database directly for processing.

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

SOAP v/s Static (In Proc) Decision?

What advantages each one has over the other are listed below.

- SOAP
  - Network Architecture
    - Outer DMZ v/s Inner DMZ for access database
  - Scalability
    - Few high end servers for rules processing
    - More low end servers for processing web requests
- Static
  - Rules Engine embedded
  - No SOAP/HTTP(s) calls, better performance

1.2.2 Universal Installation Option Integration

Oracle Adaptive Access Manager's Universal Installation Option (UIO) is a proxy-based deployment of Adaptive Risk Manager and Adaptive Strong Authenticator that requires little or no integration with enterprise applications.

A proxy intercepts site traffic and routes it through Adaptive Risk Manager Online for strong authentication and fraud detection and prevention.

1.2.3 Access Management Integration

Oracle Adaptive Access Manager is integrated or used along with an access management product. This option uses both the Adaptive Strong Authenticator and Adaptive Risk Manager Web applications.

1.2.4 SAML Integration

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

1.3 What Web Applications to Deploy?

There are many flavors of Web Application deployment for Oracle Adaptive Access Manager. The deployment you choose is based on your needs. A chart is presented below showing the combinations of each flavor of Web Application deployment.

Integration Type	Adaptive Risk Manager Web Application	Adaptive Strong Authenticator Web Application	Native
Oracle Adaptive Access Manager – Universal Installation Option See Section 1.2.2, "Universal Installation Option Integration" and "Oracle Adaptive Access Manager Proxy" in *Oracle Adaptive Access Manager Developer's Guide*.	X	X	

Integration Type	Adaptive Risk Manager Web Application	Adaptive Strong Authenticator Web Application	Native
Oracle Adaptive Access Manager – Access Management (like Oracle Access Manager, etc.) Refer to Section 1.2.3, "Access Management Integration", and for an Oracle Access Manager integration, see "Integration with Oracle Access Manager" in *Oracle Adaptive Access Manager Developer's Guide*.	X	X	
Oracle Adaptive Access Manager – SAML (e.g. SSL VPN*) Refer to Section 1.2.4, "SAML Integration."	X	X	
Oracle Adaptive Access Manager – Application (Embedded) ** See Section 1.2.1, "Native Integration" and "API Integration" in *Oracle Adaptive Access Manager Developer's Guide*.	X		X
Only Authenticators See Section 1.2.1, "Native Integration" and "API Integration" in *Oracle Adaptive Access Manager Developer's Guide*.			X

* Oracle Adaptive Access Manager is the authentication provider and uses LDAP for password authentication

** Supports with and without Authenticators

1.4 Oracle Adaptive Access Manager Architecture

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

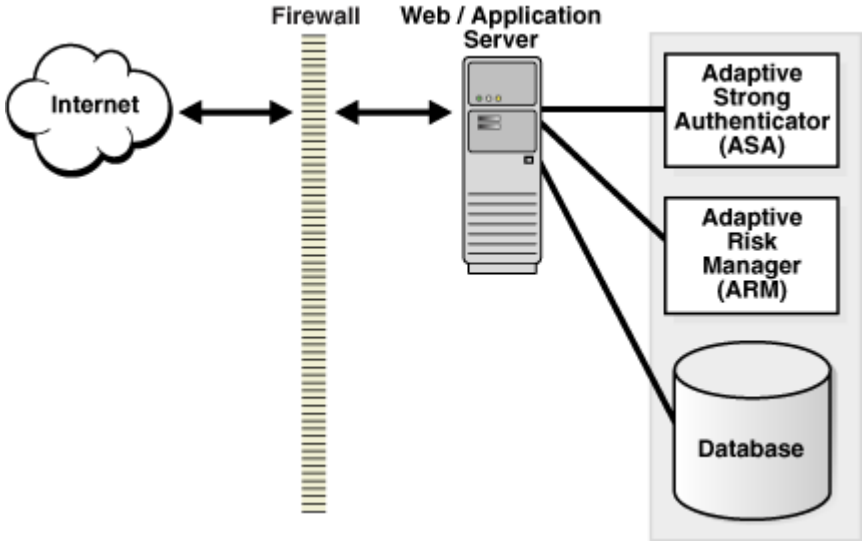
The diagram below shows the relationship between the Internet, the Web/Application Server that hosts Adaptive Risk Manager and Adaptive Strong Authenticator, and the database that stores Oracle Adaptive Access Manager's data.

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

1.4.1 Simple Architectural Scenario for Deployment

The diagram below depicts an out-of-the-box deployment. In this simple (out-of-the-box) deployment, Adaptive Strong Authenticator and Adaptive Risk Manager are on the same server.

Figure 1–1 Out-of-the-box deployment scenario

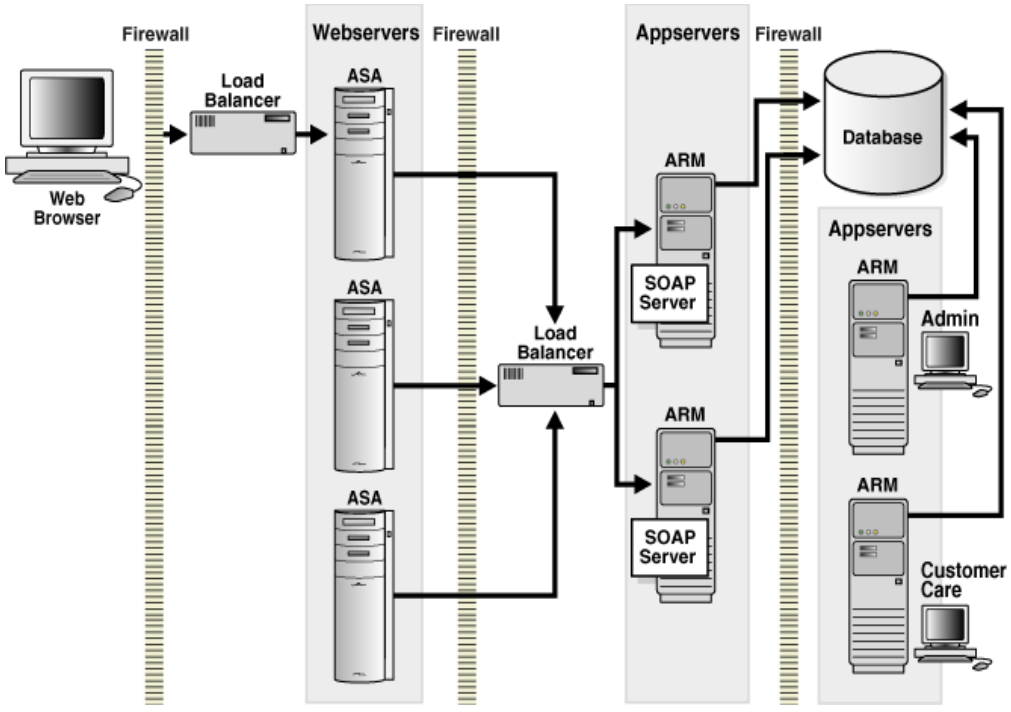


1.4.2 Recommended Architectural Scenario for Deployment

The diagram below depicts the recommended architectural scenario for deployment.

In this scenario, Adaptive Access Manager is separated for performance and scalability, and horizontal scalability for the Adaptive Risk Manager application and database.

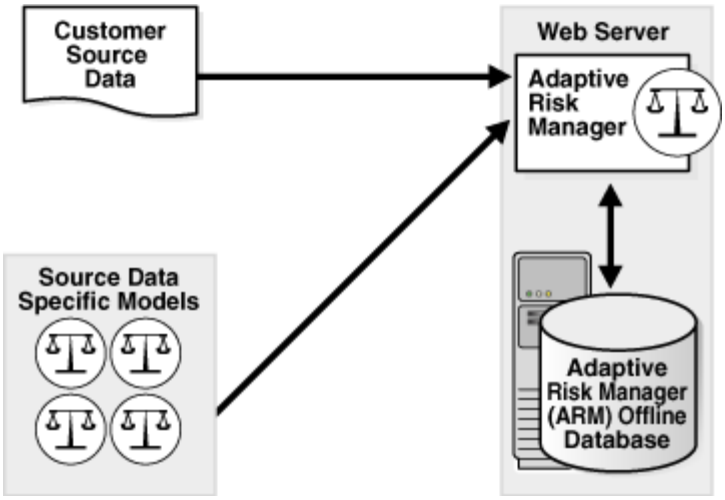
Figure 1–2 Sample deployment scenario for performance and scalability



1.4.3 Adaptive Risk Manager Offline

Adaptive Risk Manager Offline has its own database. This additional database 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.

Figure 1–3 Adaptive Risk Manager Offline Architecture



For the Adaptive Risk Manager Offline database, follow the instructions in Chapter 3, "Creating an Oracle Database Schema," or Chapter 4, "Creating a SQL Server Schema," for creating the database schema and populating it with the default values.

1.5 Installation Checklist

An installation checklist is provided below.

Task	Adaptive Risk Manager	Adaptive Strong Authenticator SOAP	Adaptive Strong Authenticator Static	Native SOAP	Native Static
Create Oracle Adaptive Access Manager database schema. Refer to Chapter 3, "Creating an Oracle Database Schema" or Chapter 4, "Creating a SQL Server Schema."	[ ]				
Create background images directory. Refer to Chapter 14, "Setting Up Background Images."	[ ]	[ ]	[ ]	[ ]	[ ]
Create log directories. Refer to Chapter 16, "Setting Up Logging."	[ ]	[ ]	[ ]	[ ]	[ ]

Task	Adaptive Risk Manager	Adaptive Strong Authenticator SOAP	Adaptive Strong Authenticator Static	Native SOAP	Native Static
Install application server. Refer to Chapter 6, "Installing Adaptive Risk Manager."	[ ]	[ ]	[ ]		
Create user roles in application server. Refer to Chapter 6, "Installing Adaptive Risk Manager" and Appendix A, "Adaptive Risk Manager User Groups."	[ ]				
Configure JNDI in application server.	[ ]		[ ]		[ ]
Unjar war file. Refer to Chapter 6, "Installing Adaptive Risk Manager."	[ ]	[ ]	[ ]	[ ]	[ ]
Configure encryption. Refer to Chapter 10, "Setting Up Encryption."	[ ]	[ ]	[ ]	[ ]	[ ]
Configure SOAP/Web services access. Refer to Chapter 11, "Configuring SOAP/Web Services Access."	[ ]	[ ]		[ ]	
Copy bharosa_server.properties.sample to bharosa_server.properties. Refer to Chapter 12, "Configuring Server Properties."	[ ]		[ ]		[ ]
Update bharosa_server.properties. Refer to Chapter 12, "Configuring Server Properties."	[ ]		[ ]		[ ]
Copy sample.sessions.xml or sample_jndi.sessions.xml to sessions.xml and update it accordingly. Refer to Chapter 13, "Configuring Database Connectivity."	[ ]		[ ]		[ ]
Copy sample.bharosa_client.properties to bharosa_client.properties. Refer to Chapter 15, "Configuring Client Properties."		[ ]		[ ]	

Task	Adaptive Risk Manager	Adaptive Strong Authenticator SOAP	Adaptive Strong Authenticator Static	Native SOAP	Native Static
Update bharosa_client.properties for ■ SOAP URL ■ Image path ■ Image URL ■ Proxy mode ■ SOAP class ■ Configuration Encryption ■ SOAP/web services access Refer to Chapter 15, "Configuring Client Properties."		[ ]		[ ]	
Update log4j.xml. Refer to Chapter 16, "Setting Up Logging."	[ ]	[ ]	[ ]	[ ]	[ ]
Rejar and deploy the war file. Refer to Chapter 6, "Installing Adaptive Risk Manager."	[ ]	[ ]	[ ]	[ ]	[ ]
Take backup of all updated files.	[ ]	[ ]	[ ]	[ ]	[ ]

If you are installing the Universal Installation Option, see "Oracle Adaptive Access Manager Proxy" in *Oracle Adaptive Access Manager Developer's Guide*.

If you are planning to install Adaptive Risk Manager Offline, refer to Chapter 8, "Installing and Configuring Adaptive Access Manager Offline."

If you are planning to load IP location data, see "IP Location Data Import" in *Oracle Adaptive Access Manager Reference Guide*.

1.6 Validation Checklist

A validation checklist is provided below.

Task	Adaptive Risk Manager	Adaptive Strong Authenticator SOAP	Adaptive Strong Authenticator Static	Native SOAP	Native Static
Start the Application Server.	[ ]	[ ]	[ ]	[ ]	[ ]
Log into Adaptive Risk Manager.	[ ]				
Import Base Models.	[ ]				
Import Rule Conditions.	[ ]				

Task	Adaptive Risk Manager	Adaptive Strong Authenticator SOAP	Adaptive Strong Authenticator Static	Native SOAP	Native Static
Import Base Questions.	[ ]				
Go to Adaptive Strong Authenticator URL and try to log in.		[ ]	[ ]		
Enable phase 2 scenarios by adding default user group to Phase2 pre- and post-authentication business models.	[ ]				
Check log file for errors.	[ ]	[ ]	[ ]	[ ]	[ ]

Adaptive Strong Authenticator (oaam_sample_models_for_asa_integration.zip) and SAMPLE (oaam_sample_models_for_native_integration.zip) models should not be imported into the same application. The models and rules are for different flows and need different sets of properties. Adaptive Strong Authenticator models are used for all Universal Installation Option-based integration/deployment. Examples for Universal Installation Option deployments are integrations with Oracle Access Manager, Site Minder, SAML, and so on. The SAMPLE models are used for native integrations where the users want to use their own user flows

2

Preparing for the Installation

The prerequisites and dependencies for the installation and configuration of Adaptive Risk Manager Online and Offline are summarized in this chapter.

This chapter contains the following topics:

2.1 Getting Started

This section contains information about the package contents of Oracle Adaptive Access Manager and the requirements to run it.

2.1.1 Package Contents

Oracle Adaptive Access Manager is packaged in a ZIP file named oaam_bin.zip.

This file contains a set of ZIP files, which are described in the table below.

Extract oaam_bin.zip to begin the Oracle Adaptive Access Manager installation.

Filename	Description
Auth_EntityDefinition.zip	Contains the entity definitions. To use Auto-learning, you must first import the required entities into the system.
oaam_base_models.zip	Contains the base business and security rules to be used in all deployments though they are specifically built for Universal Install Option flows.
oaam_bireports_oradb.zip	Contains globalization information, templates and other files needed to generate Oracle BIP reports.
oaam_cli.zip	Contains the command line interface utility for import and export of models/rules/questions and so on. Not for use with geolocation data.
oaam_db_patch_10.1.4.5.zip	Used for upgrade
oaam_kba_questions_<locale>.zip and oaam_kba_questions_<locale>_<country>.zip	Contains challenge questions. The locale-specific zip file must be imported for successful registration and log in for Adaptive Strong Authenticator.
oaam_keystore_util.zip	Contains the encryption scripts.
oaam_legacy_rule_templates.zip	Contains rule templates that were shipped out in previous releases. This package is used for upgrades.
oaam_location_etl.zip	Contains the geolocation data loader utility.

Filename	Description
oaam_native_inproc.zip	Used for JAVA static linked integration deployments
oaam_native_soap.zip	Applications using embedded server calls using SOAP/Web services. Used for native JAVA integration deployments only.
	Note: The sample application sources should not be installed in production. They are used only as a reference.
oaam_oam_plugins.zip	Authentication plug-in for Oracle Access Manager. Apply this patch after installation of Adaptive Risk Manager and Adaptive Strong Authenticator.
oaam_rhel4_apache_uio.zip	Contains the proxy module and supporting libraries for Apache httpd for RHEL4
oaam_rm_online.zip	Adaptive Risk Manager Online WAR file.
oaam_rm_offline.zip	Adaptive Risk Manager Offline WAR file.
oaam_rule_conditions.zip	Contains a library of pre-configured conditions
oaam_sa_inproc.zip	The Adaptive Strong Authenticator WAR file for static installations. (For installations not using Adaptive Risk Manager as SOAP Server.)
oaam_sa_soap.zip	The files used for native integrations, i.e. non-static. (For installations not using Adaptive Risk Manager as SOAP Server.)
oaam_win_apache_uio.zip	Contains the proxy modules and libraries for Apache httpd for Microsoft Windows
oaam_win__isa_uio.zip	Contains proxy DLL for the Microsoft ISA.
oracle_rm_database_setup.zip	Oracle database scripts for new installation of 10.1.4.5.
sample_bg_images.zip	Contains sample library of personalization images to be used as a placeholder. Customers who have purchased Oracle Adaptive Access Manager may contact Oracle Support for a full library of background images.
sqlserver2005_database_setup.zip	Contains SQL database scripts for new installation of 10.1.4.5.

2.1.2 Supported Configurations

This section contains information about the requirements to run Oracle Adaptive Access Manager.

RAM

2.0 GB or higher

Database Versions

- Oracle 10g or later
- Microsoft SQL Server 2005 SP1, SP2

Application Servers

- WebLogic Server 9.x, 10.x (Sun JDK 1.5.x or higher)
- WebSphere 5.1 and 6.1 (IBM JDK 1.4.2 SR 06, SR09)
- Tomcat 5.5x or higher

Software

- JDK 1.4 or later

- JDBC driver

Operating Systems

- Redhat 8.0, 9.0. AS 2.1, ES 3.0, ES 4.0
- Windows 2003
- Solaris 10
- HP-UX
- AIX 4.3.3, 5.2, 5.3

Oracle Adaptive Access Manager Proxy

If using the Oracle Adaptive Access Manager Proxy: Microsoft Internet Security and Acceleration (ISA) Server 2006 Standard Edition or Apache Web server 2.2.8

2.2 Prerequisites and Dependencies

The prerequisites and dependencies for the installation and configuration of Adaptive Risk Manager Online and Offline and Adaptive Strong Authenticator are summarized in the tables below.

2.2.1 Adaptive Risk Manager Online and Offline

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

Prerequisites and Dependencies	Details
Java	Java Runtime Environment, version 1.4 or higher, needs to be installed. Environment variables JAVA_HOME and PATH must be set appropriately.
Adaptive Risk Manager Online Database	The Adaptive Risk Manager Online Server needs access to the database server that contains the Adaptive Risk Manager Online schema and it needs to be populated with some initial data. Follow the instructions in Chapter 3, "Creating an Oracle Database Schema" or Chapter 4, "Creating a SQL Server Schema," for creating the Adaptive Risk Manager Online schema and populating it with the default values. Note: Any failover, clustering, and replication technology for the database is supported in Adaptive Risk Manager Online. If you are using the Microsoft SQL server database, to load data to the database, sqljdbc.jar should be copied to a third-party directory.
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 Chapter 3, "Creating an Oracle Database Schema" or Chapter 4, "Creating a SQL Server Schema" for creating the database schema and populating it with the default values.

Prerequisites and Dependencies	Details
File Write Permission	The Adaptive Risk Manager Online and Offline Server writes activity logs to rolling log files. The verbosity of the logs can optionally be configured using a standard log4j.xml configuration. For more information on setting up logging, refer to Chapter 16, "Setting Up Logging."
Shared Images Directory (for Adaptive Risk Manager Online)	If personalized authentication devices are used, it is recommended that all Adaptive Risk Manager Online Application Servers have access to the directories containing the images and that they be on a shared drive If this is not feasible, duplicate the image files on each server. Note that the base paths must be identical on all machines that will render the images, including the client applications. For more information on setting up background images, refer to Chapter 14, "Setting Up Background Images."
Port Configuration	Ensure that the port used by the Adaptive Risk Manager Online or Offline Application Server is accessible to the client machine (the application integrating with Adaptive Risk Manager, not the end-user client machine). You are allowed to configure the port number.
JVM Settings for Adaptive Risk Manager Online	The Minimum Memory setting is 1024 MB. For high volume deployments, perform load testing to come up with ideal settings.
IP Intelligence License for Adaptive Risk Manager Online	Adaptive Access Manager integrates with numerous IP Intelligence products due to our open API's. Common IP Intelligence products include: ■ Quova ■ IP2Location ■ MaxMind

TCP/IP Parameters for Adaptive Risk Manager Online	For windows based deployments, the following TCP/IP parameters are highly recommended:
	`[HKEY_LOCAL_`
	`MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\`
	`TcpTimedWaitDelay= 1e`
	`MaxUserPort = ffff`

2.2.2 Adaptive Strong Authenticator

The prerequisites and dependencies for the installation and configuration of Adaptive Strong Authenticator are summarized in the table below.

Prerequisites and Dependencies	Descriptions
Shared Images Directory	If personalized authentication devices are used, it is recommended that you provide the application servers and the Adaptive Risk Manager Online server with access to the directories containing the images on a shared drive. The sample_bg_images.zip contains sample images for TextPad. Unzip the images to the Webapp root folder and then point the bharosa.image.dirlist property in bharosa_client.properties and in bharosa_server.properties to this folder. In Adaptive Strong Authenticator, the property file is bharosa_client.properties. In Adaptive Risk Manager, the property file is bharosa_server.properties. The files are located in the <webapps_install_directory>/<webapps_name>/WEB-INF/classes directory.
Port Configuration	The Adaptive Strong Authenticator server must be able to access the Adaptive Risk Manager server via HTTP/HTTPS.

3

Creating an Oracle Database Schema

The Oracle Adaptive Access Manager Application Server, which hosts Adaptive Risk Manager and Adaptive Strong Authenticator products needs access to the database server that contains the Adaptive Access Manager schema and it needs to be populated with some initial data.

The creation of the database schema is the same for both Adaptive Risk Manager Online and Offline.

You can install the Adaptive Access Manager schema in either an Oracle database or a SQL Server.

If you are planning to install the schema in SQL Server 2005, skip this chapter and go to Chapter 4, "Creating a SQL Server Schema."

> **Note:** If you are planning a proxy installation, you must install the Adaptive Manager Access Manager schema first before proceeding to the proxy installation.

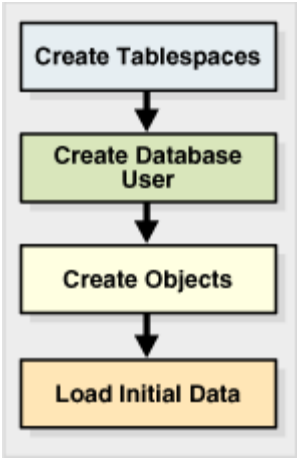
This chapter contains the following topics:

3.1 Installation Steps Overview

This chapter contains the steps needed to create the Adaptive Access Manager schema in an Oracle database.

The database used must be 10g or higher.

An Oracle Enterprise Edition database is recommended.



3.2 Database Character Set

This section contains information if you are planning to use Oracle Adaptive Access Manager for non-English setup.

New Database

If you plan to use Oracle Adaptive Access Manager for non-English setup (i.e., localized), specify a unicode character set for your database during the Oracle database installation. For example, AL32UTF8.

Existing Database

If you plan to use Oracle Adaptive Access Manager for non-English setup and you want to use an existing database for your Oracle Adaptive Access Manager repository, determine its database character set before proceeding with the setup.

To find out the current database character set, run the following SQL script with DBA credentials:

```
select value from NLS_DATABASE_PARAMETERS where parameter='NLS_CHARACTERSET' and
value like '%UTF8%'
```

The above query should return at least 1 row if the database character is set to UTF8.

If you are not using a unicode character set, refer to Metalink article #225938.1, "Database Character Set Healthcheck," for upgrade instructions.

3.3 Oracle Initialization Parameters

Ensure that the appropriate initialization parameters are set before you create your database schema within the Oracle database. Please refer to the Notes section for additional details about setting the initialization parameters.

1. Set the initialization parameters.

```
ALTER SYSTEM SET db_writer_processes=4 SCOPE=SPFILE;
ALTER SYSTEM SET fast_start_mttr_target=300 SCOPE=SPFILE;
ALTER SYSTEM SET open_cursors=2000 SCOPE=SPFILE;
ALTER SYSTEM SET pga_aggregate_target=512M SCOPE=SPFILE;
ALTER SYSTEM SET processes=500 SCOPE=SPFILE;
ALTER SYSTEM SET query_rewrite_enabled='FALSE' SCOPE=SPFILE;
ALTER SYSTEM SET sessions=500 SCOPE=SPFILE;
```

```
ALTER SYSTEM SET shared_pool_size=500M SCOPE=SPFILE;
ALTER SYSTEM SET timed_statistics=TRUE SCOPE=SPFILE;
ALTER SYSTEM SET undo_management='AUTO' SCOPE=SPFILE;
ALTER SYSTEM SET undo_retention=900 SCOPE=SPFILE;
ALTER SYSTEM SET session_cached_cursors=500 SCOPE=SPFILE;
ALTER SYSTEM SET commit_write='BATCH,NOWAIT' SCOPE=SPFILE;
```

The following initialization parameter must be set for a RAC-specific environment:

```
max_commit_propagation_delay=0 (Only for RAC-specific environment)
```

See the *Oracle Database Administrator's Guide* for information about setting initialization parameter values in 10g.

Please refer to the appropriate documentation for release-specific limitations.

2. Restart the database after setting all the values.

Notes

The following notes are provided for your reference.

- undo_retention parameter value

  Adjust the undo_retention parameter value as per the UNDO tablespace size and the size of the flash recovery area.

- commit_write initialization parameter

  For 10g and earlier, the commit_write initialization parameter must be set to "BATCH,NOWAIT." Keeping the default value "IMMEDIATE,WAIT" will cause contention at the database level, which affects the performance of the system.

  For 11g, set the commit_write initialization parameter to "NOWAIT."

3.4 Running the Scripts

To create the Adaptive Access Manager tables and populate the schema with the required objects, follow the procedures provided below.

The database scripts are located in oaam_db/full_schemas/oracle_rm_database_setup.zip

The database scripts for databases with the partition feature are located in oaam_db/full_schemas/oracle_partition_rm_database_setup.zip. For information on the partition tables and scripts to maintain the partition, refer to Section 3.7, "Partition Reference."

Unzip the file into a folder of your choice. For example, oaam_db.

The database password is set when you run the db_setup.sql script and you're prompted for a username and password.

3.4.1 Windows

For the Windows operating system, create the Adaptive Access Manager tables and populate the schema by following the procedures provided below:

1. Start SQL*Plus.

   Start > Programs > Oracle_Database_Edition > Run SQL Command Line.

2. When the SQL*Plus Command Line appears, enter

```
connect
```

3. When prompted, enter the user name and password of a DBA privileged user.

   For example, D:/>sqlplus sys/manager as sysdba

4. Run the `db_setup.sql` database script from the location of the scripts.

   For example,

   ```
   SQL > @E:/oaam_db/db_setup.sql
   ```

3.4.2 UNIX

For the UNIX operating system, create the Adaptive Access Manager tables and populate the schema by following the procedures provided below:

1. Login to your server.
2. Run the following command:

   ```
   sqlplus "sys as sysdba"
   or
   sqlplus "/ as sysdba"
   ```

3. Run the `db_setup.sql` database script from the location of the scripts.

   For example,

   ```
   SQL > @/home/oracle/oaam_db/db_setup.sql
   ```

3.5 Setup Prompts

When the scripts are run, they will prompt you for:

- the directory location for the data tablespace

  For example, in Windows, e:\oraclexe\oradata\xe

  For example, in UNIX, /home/oracle/oradata

  Note: The directory must already have been created.

- the directory location for the index tablespace

  For example, in Windows, e:\oraclexe\oradata\xe

  For example, in UNIX, /home/oracle/oradata

- a username

  For example, oaamdbuser

- a password for the database user

  For example, abcd1234

- the temporary tablespace to be used.

  For example, TEMP

3.6 Scripts

The scripts that will be run are listed below. The SQL command window will close automatically when the scripts complete their run.

3.6.1 db_setup.sql

When you run the db_setup.sql script, it will automatically run all the other scripts; there is no need to run the scripts manually unless you encounter a problem.

Please make sure the database user can create files on the operating system during tablespace creation. The file permissions should be set properly.

Also, ensure that the script creates the specified number of tables and indexes.

You should see a message:

```
OAAM No. of tables should be XXX and the script created tables: YYY
```

XXX should be equal to YYY

3.6.2 cr_vcrypt_tbs.sql

This script creates two tablespaces (BRSADATA, BRSAINDX) required for Adaptive Access Manager.

Depending on the volume of transactions expected, this script needs to be updated for the tablespace size.

3.6.3 cr_vcrypt_usr.sql

This script is called by db_setup.sql to create the Oracle Adaptive Access Manager repository user and grants it the appropriate privileges.

3.6.4 cr_vcrypt_obj.sql

This script is called by db_setup.sql to create the objects in the Oracle Adaptive Access Manager repository such as tables, sequences and constraints.

3.6.5 Seed Data Initialization Steps

The initialization process involves the scripts listed below. The db_setup.sql calls the following during the first-time setup of the Oracle Adaptive Access Manager repository.

The scripts are run using the Oracle Adaptive Access Manager repository user, for example, BRSAADMIN.

- oracle_user_init.sql
- oracle_policy_init.sql
- oracle_default_locales.sql
- oracle_answerhints.sql
- oracle_bharosaconfig.sql
- oracle_scoringpolicy.sql
- oracle_validations.sql

The user is not required to run these scripts. The db_setup.sql script will run them.

Note: Be sure to check the log files for any errors when running the scripts.

3.6.5.1 oracle_user_init.sql

The oracle_user_init.sql script populates the default data set.

3.6.5.2 oracle_policy_init.sql

The oracle_policy_init.sql script will populate the default data set.

3.6.5.3 oracle_default_locales.sql

The oracle_default_locales.sql script will populate the locale table with seed data.

3.6.5.4 oracle_answerhints.sql

The oracle_answerhints.sql script will populate the default answer hints set.

3.6.5.5 oracle_bharosaconfig.sql

The oracle_bharosaconfig.sql script will populate the Oracle Adaptive Access Manager configuration table with the Oracle Adaptive Access Manager configuration.

3.6.5.6 oracle_scoringpolicy.sql

The oracle_scoringpolicy.sql script will populate the seed data for challenge question scoring.

3.6.5.7 oracle_validations.sql

The oracle_validations.sql script will populate the seed data for the validation of the challenge questions.

3.7 Partition Reference

Database tables in the Oracle Adaptive Access Manager database are divided into three different categories. The composite partition (RANGE,HASH) is in all the tables. The Range partition is created using CREATE_TIME while the HASH key is defined as per application logic.

3.7.1 Tables

Details about partitioned and non-partitioned tables are provided below.

3.7.1.1 Static Partition Tables

Frequency: Monthly

Tables:

- V_USER_QA
- V_USER_QA_HIST

3.7.1.2 Transactional Partition Tables

Frequency: Monthly

Tables:

- VCRYPT_TRACKER_NODE_HISTORY
- VCRYPT_TRACKER_USERNODE_LOGS
- VCRYPT_TRACKER_NODE
- VT_USER_DEVICE_MAP
- V_MONITOR_DATA
- VT_ENTITY_ONE
- VT_ENTITY_ONE_PROFILE
- VT_USER_ENTITY1_MAP
- VT_ENT_TRX_MAP
- VT_TRX_DATA
- VT_TRX_LOGS

Frequency: Weekly

Tables:

- VR_POLICYSET_LOGS
- VR_POLICY_LOGS
- VR_RULE_LOGS
- VR_MODEL_LOGS
- VT_SESSION_ACTION_MAP

Other than the tables mentioned above, all other tables are non-partitioned.

3.7.2 Partition Maintenance Scripts

After the initial Oracle Adaptive Access Manager Repository setup, use the following scripts to maintain the partition.

3.7.2.1 Add_Monthly_Partition_tables.sql

This script should be used to add partitions for tables with the Monthly frequency.

The script should be run at the end of each month to create partitions for the following month. To add partitions for subsequent months at the same time, run this script multiple times; when you run the script multiple times, partitions are added based on their previous month's partition.

If you fail to run the script to create monthly partitions (if your monthly partition is missing), the database errors, "ORA-14400" and "ORA-14401," are encountered, forcing the Oracle Adaptive Access Manager application to stop.

To avoid errors, it is recommend that you schedule this script as an automated job.

3.7.2.2 Add_Weekly_Partition_tables.sql

This script should be used to add partitions for tables with the Weekly frequency.

The script should be run at the end of each month to create partitions for the following week. To add partitions for subsequent weeks at the same time, run this script multiple

times; when you run the script multiple times, partitions are added based on their previous week's partition.

If you fail to run the script to create weekly partitions (if your weekly partition is missing), the database errors, "ORA-14400" and "ORA-14401," are encountered, forcing the Oracle Adaptive Access Manager application to stop.

To avoid errors, it is recommend that you schedule this script as an automated job.

3.7.2.3 Drop_Monthly_Partition_tables.sql

This script should be used to drop partitions for tables with the Monthly frequency. This script should run at the end of each month to drop partitions older than sixth months as per the Oracle Adaptive Access Manager Application requirement. Eventually, these tables will have six partitions at any point of time.

3.7.2.4 Drop_Weekly_Partition_tables.sql

This script should be used to drop partitions for tables with the Weekly frequency. This script should run at the end of every fourteenth day or third week from the start of the Oracle database creation to the dropping of partitions older than two weeks as per the Oracle Adaptive Access Manager application requirement.

4

Creating a SQL Server Schema

The Oracle Adaptive Access Manager Application Server which hosts Adaptive Risk Manager and/or Adaptive Strong Authenticator products needs access to the database server that contains the Oracle Adaptive Access Manager schema and it needs to be populated with some initial data.

The creation of the database schema is the same for both Adaptive Risk Manager Online and Offline.

You can install the Oracle Adaptive Access Manager schema in either an Oracle database or a SQL Server 2005.

If you are planning to install the schema in an Oracle database, go to Chapter 3, "Creating an Oracle Database Schema."

> **Note:** If you are planning a proxy installation, you must install the Adaptive Manager Access Manager schema first before proceeding to the proxy installation.

This chapter provides the steps and information about the scripts to be run for installation and initialization of the Oracle Adaptive Access Manager Database on SQL Server 2005.

This chapter contains the following topics:

4.1 Prerequisites

The scripts for installing and initializing the Oracle Adaptive Access Manager database are located in oaam_db/full_schemas/sqlserver2005_database_setup.zip.

For a database with globalization support, the scripts are located in oaam_db/full_schemas/sqlserver2005_globalized_database_setup.zip.

Ensure the following pre-installation tasks have been completed before you install and initialize your database.

1. Create the directories for the database files. For example: x:\sqldata.

2. Update the 010_cr_bharosa_db.sql with the directory path for the database using the same path that you used in step 1.
3. Optionally, you can change the database name. If you change the name, you need to update all the files manually for the new database. The default database name is bharosa_db.

4.2 Installation Steps

Installing and initializing the Oracle Adaptive Access Manager Database schema is a three-step process.

Refer to Section 4.1, "Prerequisites" to ensure that you have completed the preliminary steps before using the scripts.

The steps for installing and initializing the Oracle Adaptive Access Manager Database are:

1. Create Database
2. Create Login
3. Load Initialization Data

4.3 Scripts

The following SQL scripts will be used to set up the database for the Oracle Adaptive Access Manager Database. Use the SQL Server Management Console to run the scripts in the order presented below.

4.3.1 Create Database

010_cr_bharosa_db.sql - This script creates the bharosa_db database. Modify the location of data file prior to executing this script.

4.3.2 Create Login

020_cr_bharosa_db_login.sql - This script creates the database user called brsamain and grants the appropriate privileges.

Note: Update the script for the password in order to set a non-default password.

4.3.3 Load Initialization Data

The scripts to load initialization data are listed below.

- 040_mssql_user_init.sql - This script populates the user group as part of the database initialization.
- 050_mssql_policy_init.sql - This script creates the default policy and policy set as part of the data base initialization process.
- 055_mssql_default_locales.sql - This script populates the locale table with seed data.
- 070_mssql_scoringpolicy.sql - This script will populate the seed data for challenge question scoring.

- 080_mssql_answerhints.sql - This script will populate the default answer hints set.
- 090_mssql_validations.sql-This script will populate the seed data for the validation of the challenge questions.
- 100_mssql_bharosaconfig.sql - This script will populate the Oracle Adaptive Access Manager configuration table with the Oracle Adaptive Access Manager configuration.

4.4 Database Properties

The recommended properties to be set at the Instance Level are

Advanced

- Number of Locks: 5000000
- Max Degree of Parallelism: 1

Processors:

- Maximum Worker Threads: 255

5

Loading IP Location Data

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

For information on importing the IP location data into the Adaptive Risk Manager Online and Offline databases, see "IP Location Data Import" in *Oracle Adaptive Access Manager Reference Guide.*

6

Installing Adaptive Risk Manager

Adaptive Risk Manager is certified with the following servers.

- WebLogic Application Server 9.x, 10.x
- Apache Tomcat Web server 5.5x or higher
- IBM WebSphere Application Server 5.1, 6.1

> **Note:** For a Microsoft SQL database, to support various functionalities of Adaptive Risk Manager, the SQL Server JDBC driver (sqljdbc.jar) from Microsoft Corporation, and the mail.jar and activation.jar from Sun Microsystems must be downloaded and placed into the oarm/WEB-INF/lib directory

The chapter provides guidelines on deploying Adaptive Risk Manager on the certified servers.

> **Note:** If you are using WebLogic, Tomcat, or WebSphere, we assume that the server has already been installed and the JNDI or JDBC data source configured.

6.1 Creating Groups/Roles

For information about groups/roles and permissions, refer to Appendix A, "Adaptive Risk Manager User Groups."

1. For the application and Web servers, the creation of groups/roles is expected. If the groups/roles do not already exist, create them. For example,
   - For Tomcat:
     - web_CSR
     - web_CSRManager
     - web_CSRInvestigator
     - web_Investigator
     - web_InvestigationManager
     - web_RuleAdministrators
     - web_EnvAdmin
     - web_SOAPServices

- For WebLogic and WebSphere:
  - CSRGroup
  - CSRManagerGroup
  - CSRInvestigator
  - Investigator
  - InvestigationManager
  - RuleAdministratorsGroup
  - EnvAdminGroup
  - SOAPServicesGroup

2. You will need to assign users to these groups/roles.

6.2 Deployment on the Application and Web Servers

Guidelines for installing Adaptive Risk Manager web application on certified Application and Web Servers are provided below.

6.2.1 WebLogic

To install the Adaptive Risk Manager web application in the WebLogic Application Server

1. Create a webapps directory.
2. Under the webapps directory, create an oarm directory.
3. Unzip oaam_rm_online.zip in the oaam_rm_online directory. The oaam_rm_online.zip file is located in the oaam_rm_online directory.
4. Copy oarm.war from the oaam_rm_online/wars directory to the webapps/oarm directory.
5. Extract the oarm.war file in the oarm directory using jar -xvf.

   For example, in UNIX: jar -xvf ~/oaam_rm_online/oarm/oarm.war

   For example, in Windows: jar -xvf e:/oaam_rm_online/oarm/oarm.war
6. Set up encryption. Refer to Chapter 10, "Setting Up Encryption."
7. Set up Adaptive Risk Manager SOAP/Web Services access. Refer to Section 11.1, "Adaptive Risk Manager SOAP/Web Services Set Up."
8. Copy sample.sessions.xml or sample_jndi.sessions.xml into sessions.xml. The sample sessions.xml files are located under the oarm/WEB-INF/classes/ directory.

   Ensure that the sessions.xml is spelled correctly. If the name is not correct, you will not be able to connect to the database.
9. Configure sessions.xml to use the JNDI or JDBC data source.

   Note: JNDI is recommended.

   For more information, refer to Chapter 13, "Configuring Database Connectivity."

10. Configure log4j.xml for logging. The file is located under the directory, oarm/WEB-INF/classes/.

    For more information, refer to Chapter 16, "Setting Up Logging."

11. Copy bharosa_server.properties.sample to bharosa_server.properties, and update the bharosa_server.properties file. The bharosa_server.properties.sample file is located under the directory, oarm/WEB-INF/classes/.

    For more information, refer to Chapter 12, "Configuring Server Properties."

12. Deploy Adaptive Risk Manager on the Application Server.

    During deployment procedure, you will need to select the exploded archive directory, oarm, to install the Adaptive Risk Manager web application.

    For detailed information on installing a web application, refer to the WebLogic documentation.

13. Log in to Adaptive Risk Manager to begin using it.

    For more information, refer to Chapter 20, "What to Do Next."

6.2.2 Tomcat

To install the Adaptive Risk Manager web application in the Tomcat Web Server

1. Under the webapps directory, create an oarm directory.
2. Unzip oaam_rm_online.zip in the oaam_rm_online directory. The oaam_rm_online.zip file is located in the oaam_rm_online directory.
3. Copy oarm.war from the oaam_rm_online/wars directory to the webapps/oarm directory.
4. Extract the oarm.war file in the oarm directory using jar -xvf.

    For example, in UNIX: jar -xvf ~/oaam_rm_online/oarm/oarm.war

    For example, in Windows: jar -xvf e:/oaam_rm_online/oarm/oarm.war
5. Set up encryption. Refer to Chapter 10, "Setting Up Encryption."
6. Set up Adaptive Risk Manager SOAP/Web Services access. Refer to Section 11.1, "Adaptive Risk Manager SOAP/Web Services Set Up."
7. Copy sample.sessions.xml or sample_jndi.sessions.xml into sessions.xml. The sample sessions.xml files are located under the oarm/WEB-INF/classes/ directory.

    Ensure that the sessions.xml is spelled correctly. If the name is not correct, you will not be able to connect to the database.
8. Configure sessions.xml to use the JNDI or JDBC data source.

    Note: JNDI is recommended.

    For more information, refer to Chapter 13, "Configuring Database Connectivity."
9. Configure log4j.xml for logging. The file is located under the oarm/WEB-INF/classes/ directory.

    For more information, refer to Chapter 16, "Setting Up Logging."

10. Copy bharosa_server.properties.sample to bharosa_server.properties, and update the bharosa_server.properties file. The bharosa_server.properties.sample file is located under the oarm/WEB-INF/classes/ directory.

    For more information, refer to Chapter 12, "Configuring Server Properties."

11. Log in to Adaptive Risk Manager to begin using it.

    For more information, refer to Chapter 20, "What to Do Next."

6.2.3 WebSphere

To deploy the Adaptive Risk Manager web application in the WebSphere Application Server

1. Under the webapps directory, create an oarm directory.
2. Unzip oaam_rm_online.zip in the oaam_rm_online directory. The oaam_rm_online.zip file is located in the oaam_rm_online directory.
3. Copy oarm.war from the oaam_rm_online/wars directory to the webapps/oarm directory.
4. Extract the oarm.war file in the oarm directory using jar -xvf.

    For example, in UNIX: jar -xvf ~/oaam_rm_online/oarm/oarm.war

    For example, in Windows: jar -xvf e:/oaam_rm_online/oarm/oarm.war
5. Set up encryption. Refer to Chapter 10, "Setting Up Encryption."
6. Set up Adaptive Risk Manager SOAP/Web Services access. Refer to Section 11.1, "Adaptive Risk Manager SOAP/Web Services Set Up."
7. Copy sample.sessions.xml or sample_jndi.sessions.xml into sessions.xml. The sample sessions.xml files are located under the oarm/WEB-INF/classes/ directory.

    Ensure that the sessions.xml is spelled correctly. If the name is not correct, you will not be able to connect to the database.
8. Configure sessions.xml to use the JNDI or JDBC data source.

    Note: JNDI is recommended.

    For more information, refer to Chapter 13, "Configuring Database Connectivity."
9. Configure log4j.xml for logging. The file is located under the oarm/WEB-INF/classes/ directory.

    For more information, refer to Chapter 16, "Setting Up Logging."
10. Copy bharosa_server.properties.sample to bharosa_server.properties, and update the bharosa_server.properties file. The bharosa_server.properties.sample file is located under the oarm/WEB-INF/classes/ directory.

    For more information, refer to Chapter 12, "Configuring Server Properties."
11. Rejar the extracted files.
12. Deploy the Adaptive Risk Manager WAR, oarm.war, on the Application Server.

    For detailed information on installing a web application, refer to the WebSphere documentation.

13. Log in to Adaptive Risk Manager to begin using it.

    For more information, refer to Chapter 20, "What to Do Next."

7

Installing the Adaptive Strong Authenticator

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

This chapter describes how to install the Adaptive Strong Authenticator.

7.1 Deploying Adaptive Strong Authenticator

Install the Adaptive Risk Manager Online first because it contains resources that will be needed by the Adaptive Strong Authenticator.

Refer to Chapter 6, "Installing Adaptive Risk Manager" for the instructions on deployment.

7.1.1 WebLogic Application Server

To install the Adaptive Strong Authenticator web application in the WebLogic Application Server

1. Extract oasa.war from oaam_sa/oaam_sa_soap.zip.
2. Under the webapps directory, create an oasa directory and extract the oasa.war file into that directory.
3. Set up encryption. Refer to Chapter 10, "Setting Up Encryption."
4. Set up Adaptive Strong Authenticator/Native Client SOAP/Web Services. Refer to Section 11.2, "Adaptive Strong Authenticator/Native Client SOAP/Web Services Set Up."
5. Follow the instructions to edit bharosa_client.properties in Chapter 15, "Configuring Client Properties."
6. Configure the log4j.xml for logging. The file is located under the oasa/WEB-INF/classes/ directory.

   For more information, refer to Chapter 16, "Setting Up Logging."
7. Rejar the extracted files.
8. Log in to WebLogic Server Administration Console.
9. Deploy the Adaptive Risk Manager WAR, oasa.war, on the Application Server.

   For detailed information on installing a web application, refer to the WebLogic documentation.

7.1.2 Tomcat Web Server

To install the Adaptive Strong Authenticator web application in the Tomcat Web Server

1. Extract oasa.war from oaam_sa/oaam_sa_soap.zip.
2. Under the webapps directory, create an oasa directory and extract the oasa.war file into that directory.
3. Set up encryption. Refer to Chapter 10, "Setting Up Encryption."
4. Set up Adaptive Strong Authenticator/Native Client SOAP/Web Services. Refer to Section 11.2, "Adaptive Strong Authenticator/Native Client SOAP/Web Services Set Up."
5. Follow the instructions to edit bharosa_client.properties in Chapter 15, "Configuring Client Properties."
6. Configure the log4j.xml for logging. The file is located under the oasa/WEB-INF/classes/ directory.

   For more information, refer to Chapter 16, "Setting Up Logging."

7.1.3 IBM WebSphere Application Server

To deploy the Adaptive Strong Authenticator web application in the WebSphere Application Server

1. Extract oasa.war from oaam_sa/oaam_sa_soap.zip.
2. Under the webapps directory, create an oasa directory and extract the oasa.war file into that directory.
3. Set up encryption. Refer to Chapter 10, "Setting Up Encryption."
4. Set up Adaptive Strong Authenticator/Native Client SOAP/Web Services. Refer to Section 11.2, "Adaptive Strong Authenticator/Native Client SOAP/Web Services Set Up."
5. Follow the instructions to edit bharosa_client.properties in Chapter 15, "Configuring Client Properties."
6. Configure the log4j.xml for logging. The file is located under the oasa/WEB-INF/classes/ directory.

   For more information, refer to Chapter 16, "Setting Up Logging."
7. Rejar the extracted files.
8. Log in to the WebSphere Administration Console.
9. Deploy the Adaptive Risk Manager WAR, oasa.war, on the Application Server.

   For detailed information on installing a web application, refer to the WebSphere documentation.

7.2 Accessing Adaptive Strong Authenticator

Refer to Section 20.4, "Logging in to Adaptive Strong Authenticator" for instructions on accessing the Adaptive Strong Authenticator.

8

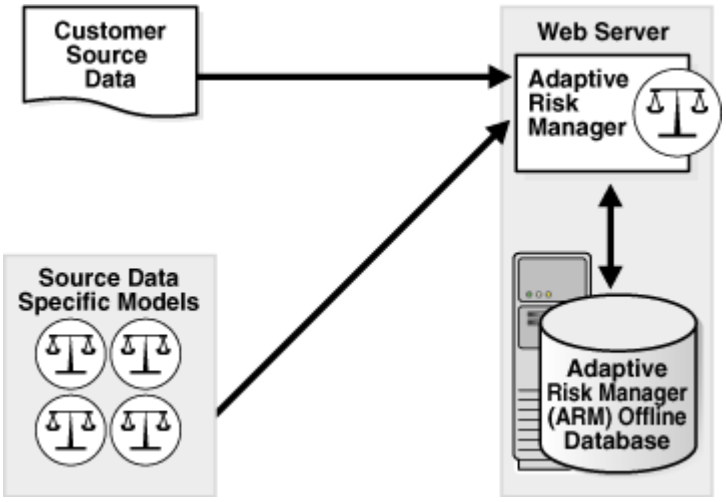
Installing and Configuring Adaptive Access Manager Offline

Note: If you do not plan to use Adaptive Risk Manager Offline, you may skip this chapter.

Adaptive Risk Manager Offline is an offline fraud analysis tool that evaluates existing transaction data for three 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 as a research and development tool to create and verify new models and rules using offline customer data without impacting customers in real-time environment.
- Thirdly, Adaptive Risk Manager Offline can be used as a supplemental offline analysis tool in the tuning of rules and verification of rules behavior against real customer data without impacting customers in real-time environment.

Figure 8–1 Adaptive Risk Manager Offline Architecture



8.1 Installation Checklist for Adaptive Risk Manager Offline

The installation and configuration of the Adaptive Risk Manager Offline is similar to the Adaptive Risk Manager Online. A table is provided below for your reference.

Task	Adaptive Risk Manager Offline
Verify prerequisites are met for offline installation	[ ]
Create Oracle Adaptive Access Manager database schema. Refer to Chapter 3, "Creating an Oracle Database Schema," or Chapter 4, "Creating a SQL Server Schema."	[ ]
Install application server. Refer to the vendor-supplied documentation for instructions on how to install the application server.	[ ]
Configure database connectivity (JNDI or JDNBC). Refer to Chapter 13, "Configuring Database Connectivity."	[ ]
Unzip oaam_rm_offline.zip.	[ ]
Under the webapps directory, create a rmoffline folder.	[ ]
Unjar oarm_offline.war into rmoffline folder.	[ ]
Create user roles in application server. Refer to the vendor-supplied documentation for instructions on how to create user roles. A list of the expected groups/roles is provided in Chapter 6, "Installing Adaptive Risk Manager."	[ ]
Install the Sun JDK. Go to `http://java.sun.com` Click the download link, and follow the instructions to install the Sun JDK.	[ ]
Generate KeyStore. Refer to Chapter 10, "Setting Up Encryption." The oarm_offline.zip does not include the oaam_utils directory. The file is part of oaam_bin.zip.	[ ]
Copy bharosa_server.properties.sample to bharosa_server.properties. If bharosa_server.properties.sample is not in the offline package, copy it from an online installation. Refer to Chapter 12, "Configuring Server Properties."	[ ]
Update bharosa_server.properties. Refer to Chapter 12, "Configuring Server Properties." Note: You do not need to set up the background images path.	[ ]
Copy sample.sessions.xml or sample_jndi.sessions.xml to sessions.xml and update it accordingly. Refer to Chapter 13, "Configuring Database Connectivity."	[ ]
Create log directories. Refer to Chapter 16, "Setting Up Logging."	[ ]
Update log4j.xml. Refer to Chapter 16, "Setting Up Logging."	[ ]
Copy the bharosa_app.properties file from an online installation or package. You will not need to modify this file. Note: The bharosa_app.properties file that shipped with the offline package must be replaced with the one from online.	[ ]
Rejar and deploy the war file.	[ ]
Take backup of all updated files.	[ ]
Verify that the database is running.	[ ]
Verify that the listener is running.	[ ]
Verify that the application server is running.	[ ]
Verify that the users are set up	[ ]
Verify that the connection URL, username, and password are in the sessions.xml	[ ]
Verify that Log4J is set up properly.	[ ]
Log in to Adaptive Access Manager Offline. Refer to Chapter 20, "What to Do Next."	[ ]
After logging into the application, please verify the logs for any issues.	[ ]

8.2 The Offline Database

The following sections provide best practices for the Adaptive Risk Manager Offline database.

8.2.1 Database Server with Good I/O capability

Make sure the host that runs the database server has good I/O capability. Offline processing in most cases is I/O intensive.

8.2.2 Proper Database Server Configuration

Make sure the database initialization parameters are set as per the recommendations in Section 3.3, "Oracle Initialization Parameters."

8.2.3 Database Indexes

Make sure to obtain and apply the latest Oracle Adaptive Access Manager database patch to ensure that the proper indexes are present.

8.3 What to Do After Installing Adaptive Risk Manager Offline

After you have completed the installation procedures, refer to the *Oracle Adaptive Access Manager Administrator's Guide* for information on how to use the Adaptive Risk Manager Offline to evaluate existing transaction data.

9

Installing the Proxy

Note: If you do not plan to use the Universal Installation Option, you may skip this chapter.

The Oracle Adaptive Access Manager's Universal Installation Option (UIO) offers multi-factor authentication to Web applications without requiring any change to the application code.

The Oracle Adaptive Access Manager Proxy is available for the Apache Web server and Microsoft Internet Security and Acceleration (ISA) Server.

See "Oracle Adaptive Access Manager Proxy" in the *Oracle Adaptive Access Manager Developer's Guide* for detailed information on installing and configuring the Oracle Adaptive Access Manager Proxy.

10

Setting Up Encryption

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

Because encryption is critical to successful implementation of Oracle Adaptive Access Manager, setup of the encryption environment cannot be delayed until a later time. If encryption is skipped entirely, the software may break and all data will be stored as clear text, easily readable by anyone.

In Oracle Adaptive Access Manager 10.1.4.5 and above, external files (called keystores) are used for the secure storage and management of the encryption keys. This chapter helps guide you through the creation of the keystores.

This chapter provides information for configuring Oracle Adaptive Access Manager for

- Configuration Encryption

  Adaptive Risk Manager encryption APIs are use to encrypt sensitive configuration data. By default, DESede algorithm is used with the encryption key provided during installation.

- Database Encryption

  Adaptive Risk Manager encrypts sensitive data in certain database fields. By default, DESede algorithm is used to encrypt with the encryption key provided during installation.

> **Note:** Adaptive Risk Manager uses the DESede encryption algorithm to encrypt database and configuration properties. However, Adaptive Risk Manager provides the option to change the algorithm to another one of your choice. By default, algorithm support is provided for AES, DES, and DESede.

For Adaptive Risk Manager and Adaptive Risk Manager encryption APIs to work properly, you will need to create and set up the following keystores:

- system_config.keystore

  The key used for configuration encryption is stored in this keystore.

- system_db.keystore

  The key used for database encryption is stored in this keystore.

Note: Ensure you keep a backup of the keystore and bharosa_server.properties and bharosa_client.properties files in case you should need to restore any customer specific customizations or upgrade to Adaptive Risk Manager software at a later date.

10.1 Creating a Keystore for Encrypting Configuration Values

To create a keystore for encrypting configuration values using 3DES algorithm,

1. Unzip the oaam_keystore_util.zip in the oaam_utils directory.

   The oaam__keystore_util.zip file is available from oaam_bin.zip.

2. In the keystore_util directory, create a file, for example, config_3des_key.file, and enter your encryption key (password).

   This is your key to the encryption algorithm.

   Please note that 3DES accepts any key, but it needs to be a minimum of 24 characters.

3. Copy sample.config_3des_input.properties to config_3des_input.properties.

4. Update config_3des_input.properties with the keystore password, alias password, and keyFile.

   A keystore is like a master vault that stores entries. To open the keystore, a "keystore password" is required. Each entry in the keystore is identified by an "alias." There can be multiple aliases in a keystore, each with its own password. This password is called the "alias password" and used to access/read the value that is identified with an alias.

5. Generate the keystore.

   - For Unix/Linux, run

     ```
     genkeystore.sh config_3des_input.properties
     ```

   - For Windows, run

     ```
     genkeystore.cmd config_3des_input.properties
     ```

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

   ```
   updateOrCreateKeyStore done!
   Keystore file:system_config.keystore,algorithm=DESede
   KeyStore Password=ZG92ZTEyMzQ=
   Alias Password=ZG92ZTEyMw==
   ```

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

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

   Ensure that you are using the Sun JDK and not another packaged Java version. Install the Sun JDK.

6. Note down the Keystore password and Alias Password printed on the screen. You will need to add these to the bharosa_server.properties and bharosa_client.properties.
7. Save the system_config.keystore file in your source code control system. Please take adequate security precaution while handling this file. The file contains critical password information. Make sure that only authorized personnel have read access to this file. If you lose it, Oracle Adaptive Access Manager will not be able to recover data encrypted. Also, you will need this file after installing Adaptive Strong Authenticator.
8. Copy system_config.keystore to Adaptive Risk Manager's classpath (for example, oarm/WEB-INF/classes). If Adaptive Strong Authenticator is being installed, copy system_config.keystore to Adaptive Strong Authenticator's classpath (for example, oasa/WEB-INF/classes).

   Note: Using the key generator utility, you can create two separate keystores for Adaptive Risk Manager and Adaptive Strong Authenticator.

9. Delete both the config_3des_key.file and config_3des_input.properties files.
10. Later when you update properties in oarm/WEB-INF/classes/bharosa_server.properties and oasa/WEB-INF/classes/bharosa_client.properties, you will update the following properties with the encoded passwords (from Step 6).

    ```
    bharosa.cipher.encryption.algorithm.enum.DESede_config.keystorePassword=<base64 encoded keystore password>
    bharosa.cipher.encryption.algorithm.enum.DESede_config.aliasPassword=<based64 encoded password to the alias>
    ```

    For updating the bharosa_server.properties file, refer to Chapter 6, "Installing Adaptive Risk Manager" for information about when to edit the file during the installation process and to Chapter 12, "Configuring Server Properties"for instructions on editing the file.

    For updating the bharosa_client.properties file, refer to Chapter 7, "Installing the Adaptive Strong Authenticator" for information about when to edit the file during the installation process and to Chapter 15, "Configuring Client Properties"for instructions on editing the file.

10.2 Creating a Keystore for Encrypting Database Data

To create a keystore for encrypting database data using 3DES algorithm,

1. In the oaam_utils/keystore_util directory, create a file, for example, db_3des_key.file, and enter your encryption key (password).

   This is your key to the encryption algorithm.

   Please note that 3DES accepts any key, but it needs to be a minimum of 24 characters.
2. Copy sample.db_3des_input.properties to db_3des_input.properties.
3. Update db_3des_input.properties with the keystore password, alias password, and keyFile.
4. Generate the keystore.

- For Unix/Linux, run

  ```
  genkeystore.sh db_3des_input.properties
  ```

- For Windows, run

  ```
  genkeystore.cmd db_3des_input.properties
  ```

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

```
updateOrCreateKeyStore done!
Keystore file:system_db.keystore,algorithm=DESede
KeyStore Password=ZG92ZTEyMzQ=
Alias Password=ZG92ZTEyMw==
```

5. Note down the Keystore password and Alias Password print on the screen. You will need to add these to the bharosa_server.properties.
6. Save the system_db.keystore file in your source code control system. Please take adequate security precaution while handling this file. The file contains critical password information. Make sure that only authorized personnel have read access to this file. If you lose it, Oracle Adaptive Access Manager will not be able to recover data encrypted.
7. Copy system_db.keystore to Adaptive Risk Manager's classpath. For example: oarm/WEB-INF/classes.
8. Delete both the db_3des_key.file and db_3des_input.properties files.
9. Later when you update oarm/WEB-INF/classes/bharosa_server.properties, you will add/update the following properties with the encoded passwords (from Step 5).

   ```
   bharosa.cipher.encryption.algorithm.enum.DESede_db.keystorePassword=<base64
   encoded keystore password>
   bharosa.cipher.encryption.algorithm.enum.DESede_db.aliasPassword=<based64
   encoded password to the alias>
   ```

   For updating the bharosa_server.properties file, refer to Chapter 6, "Installing Adaptive Risk Manager" for information about when to edit the file during the installation process and to Chapter 12, "Configuring Server Properties"for instructions on editing the file.

10.3 Other Procedures

For more information on defining and adding encryption schemes and creating keystores, refer to Appendix C, "Upgrading from 3.5 to 10.1.4.3."

11

Configuring SOAP/Web Services Access

For Web Services/SOAP access

- set up access for Adaptive Risk Manager Online
- set up access for Adaptive Strong Authenticator/Native Client

> **Note:** Both procedures must be performed for authentication to work.

This chapter also provides information on security recommendations and how to disable HTTP authentication for Web Services.

11.1 Adaptive Risk Manager SOAP/Web Services Set Up

Web Services/SOAP clients need to send the username and password for successful communication with Adaptive Risk Manager web services.

The password needs to be stored in a KeyStore for security.

Out-of-the-box, Adaptive Risk Manager publishes Web services at the URL: /oarm/services/. This URL is secured by HTTP authentication.

Access to this URL is allowed to the users of the "web_SOAPServices" role or "SOAPServicesGroup" group. You must add users to this role/group for access to Adaptive Risk Manager Web services. For more information about adding users to roles/groups, refer to the product-specific documentation for your chosen application/Web server.

11.2 Adaptive Strong Authenticator/Native Client SOAP/Web Services Set Up

> **Note:** Perform this procedure after Adaptive Strong Authenticator/Native Client setup.

To set up security for Adaptive Strong Authenticator/Native Client web services

1. In the oaam_utils/keystore_util directory, create a file, for example, soap_key.file, and enter the HTTP authentication user password in it. (The password from the user that was added to the "web_SOAPServices" role or "SOAPServicesGroup" group).

2. Copy sample.soap_3des_input.properties to soap_3des_input.properties.
3. Update soap_3des_input.properties with the keystore password, the alias password, and password file.

```
#This is the password for opening the keystore.
keystorepasswd=

#This is the password reading alias (key) in the keystore
keystorealiaspasswd=

#File containing from key. Please note, keys in AES could be binary. Also note
algorithms like 3DES require minimum 24 characters in the key
#keyFile=soap_key.file
keyFile=
```

4. Generate the keystore.
   - For Unix/Linux, run

     ```
     genkeystore.sh soap_3des_input.properties
     ```

   - For Windows, run

     ```
     genkeystore.cmd soap_3des_input.properties
     ```

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

```
updateOrCreateKeyStore done!
Keystore file:system_soap.keystore,algorithm=DESede
KeyStore Password=ZG92ZTEyMzQ=
Alias Password=ZG92ZTEyMw==
```

5. Note down the Keystore password and Alias Password print on the screen. You will need to add these to the bharosa_client.properties.
6. Save the system_soap.keystore file in your source code control system. Please take adequate security precaution while handling this file. The file contains critical password information. Make sure that only authorized personnel have read access to this file. If you lose it, Oracle Adaptive Access Manager will not be able to recover data encrypted.
7. Copy system_soap.keystore to the classpath of the Adaptive Strong Authenticator/Native Client deployment folder. For example: oasa/WEB-INF/classes.
8. Delete both the soap_key.file and soap_3des_input.properties files.
9. Later, when you update properties in oasa/WEB-INF/classes/bharosa_client.properties, you will add/update the following properties with the encoded passwords (from Step 5) and the authentication username.

```
vcrypt.soap.auth.keystorePassword=<base64 encoded keystore password>
vcrypt.soap.auth.aliasPassword=<based64 encoded password to the alias>
vcrypt.soap.auth.username=<user configured for accessing the soap services>
vcrypt.soap.auth.keystoreFile=system_soap.keystore
```

   For updating the bharosa_client.properties file, refer to Chapter 7, "Installing the Adaptive Strong Authenticator" for information about when to edit the file during the installation process and to Chapter 15, "Configuring Client Properties"for instructions on editing the file.

11.3 Security Recommendations

Security recommendations for Adaptive Risk Manager are listed below. We recommend that you,

- have an LDAP of user roles
- use form base authentication for Adaptive Risk Manager
- split SOAP and Adaptive Risk Manager Admin servers
- use Keystore if your Web container supports Keystores

11.4 How to Disable HTTP Authentication for Web Services

Disabling Web Services for Adaptive Risk Manager

If Web services is secured in another way and HTTP authentication is not required, take a backup, and edit web.xml in oarm/WEB-INF removing the security constraints.

An example of security constraints is shown below.

```
<!-- Comment this section, if webservices security using http athentication is not
required --
    <security-constraint>
        <web-resource-collection>
            <web-resource-name>webservice</web-resource-name>
            <url-pattern>/services/*</url-pattern>
            <http-method>GET</http-method>
            <http-method>POST</http-method>
        </web-resource-collection>
        <auth-constraint>
            <role-name>web_SOAPServices</role-name>
        </auth-constraint>
    </security-constraint>
-->
```

Note: By removing security constraints, any one with access to Adaptive Risk Manager can call Web Services and perform Web services calls.

Disabling Web Services for Adaptive Strong Authenticator/Native Client

To disable HTTP authentication for Adaptive Strong Authenticator, set vcrypt.soap.auth=false in the bharosa_client.properties file.

The bharosa_client.properties file is located in the classes directory in the Adaptive Strong Authenticator/Native client deployment folder (for example, oasa/WEB-INF/classes).

11.5 Other Procedures

For more information on defining and adding encryption schemes and creating keystores, refer to Appendix C, "Upgrading from 3.5 to 10.1.4.3."

12

Configuring Server Properties

Encryption of database data and configuration data, Multi-tenant functionality, background image access as well as other functions requires updating the bharosa_server.properties file.

12.1 Updating the bharosa_server.properties File

To modify the bharosa_server.properties file

1. Copy bharosa_server.properties.sample to bharosa_server.properties. The bharosa_server.properties.sample file is located under the oarm/WEB-INF/classes/ directory.
2. In bharosa_server.properties, update the appropriate values for the Adaptive Strong Authenticator images path.
3. Ensure that the database data encryption and configuration value encryption properties have been added.

```
bharosa.cipher.encryption.algorithm.enum.DESede_config.keystorePassword=<base64
encoded keystore password>
bharosa.cipher.encryption.algorithm.enum.DESede_config.aliasPassword=<based64
encoded password to the alias>

bharosa.cipher.encryption.algorithm.enum.DESede_db.keystorePassword=<base64
encoded keystore password>
bharosa.cipher.encryption.algorithm.enum.DESede_db.aliasPassword=<based64
encoded password to the alias>
```

   For more information, refer to Chapter 10, "Setting Up Encryption."
4. If you want the username to be in lowercase, set vcryptuser.loginid.lowercase to true.
5. Back up and secure the bharosa_server.properties file in case you should need to restore any customer specific customizations or upgrade to Adaptive Risk Manager software at a later date.

12.2 Sample Code

For your reference, sample code is provided below.

```
#this is to point to the shared image directory, both bharosa_client.properties
and bharosa_server.properties
#should point to the same value
bharosa.image.dirlist=/bharosa_images/allpads/textpad/
```

13

Configuring Database Connectivity

TopLink is an object-relational mapping (ORM) package for Java developers. Oracle Adaptive Access Manager uses TopLink for database connectivity. You must configure `sessions.xml` to use TopLink in order to connect to your Adaptive Risk Manager Online or Offline database.

For information on configuring your database connectivity for JDBC, refer to the "Configuring sessions.xml for JDBC" section; for information on configuring your database connectivity for JNDI, refer to the "Configuring sessions.xml for JNDI" section.

If you are using the Tomcat Web server, follow the procedure documented in the "Configuring sessions.xml for JDBC" section.

13.1 Configuring sessions.xml for JDBC

To configure sessions.xml for JDBC

1. Copy your sample.sessions.xml reference file into a sessions.xml file. The sample.sessions.xml is located under the /WEB-INF/classes directory.
2. Modify the following tags with the appropriate values. Refer to "sessions.xml Tags for JDBC" for more information.
   - <platform-class>
   - <driver-class>
   - <connection-url>
   - <user-name>
   - <password>
   - <connection-pools>

13.1.1 sessions.xml Tags for JDBC

How to modify the tags is explained below.

<platform-class>

Refer to "TopLink platform-class" for the platform specific property that you will modify the TopLink <platform-class> tag with.

<driver-class>

If you are using an Oracle 10g driver, specify the JDBC driver class. An example in bold type is provided in the "sessions.xml File Sample for JDBC" section.

<connection-url>

The connection URL is given as "jdbc:oracle:thin:@%hostname%:%port%:%database sid%." An example in bold type is shown in the "sessions.xml File Sample for JDBC" section below.

<user-name>

Specify the username for the database account.

<password>

Specify the password for the database account.

> **Note:** The password can be a TopLink encrypted password.

To encrypt the password, using the following command:

For Windows:

```
java -classpath "vcrypt.jar;toplink.jar"
com.bharosa.vcrypt.utility.cmdline.BharosaCmdLine -toplink-password-encrypt
mydbpassword
```

For UNIX:

```
echo "mydbpassword" | $JAVA_HOME/bin/java -classpath
./vcrypt.jar:./toplink.jar:./log4j-1.2.9.jar
com.bharosa.vcrypt.utility.cmdline.BharosaCmdLine -toplink-password-encrypt
```

<connection-pools>

For performance reasons, make sure that the `max-connections` and the `min-connections` are set to the same value for the <read-connection-pool> and the <write-connection-pool>.

13.1.2 sessions.xml File Sample for JDBC

For your reference, a `sessions.xml` file is provided below.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <toplink-sessions version="10g Release 3 (10.1.3.1.0)"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
- <session xsi:type="server-session">
  <name>default</name>
  <event-listener-classes />
  <primary-project xsi:type="xml">BharosaTLMappings.xml</primary-project>
- <login xsi:type="database-login">

<platform-class>oracle.toplink.platform.database.oracle.Oracle10Platform</platform
-class>
<user-name>%username%</user-name>
<password>%password%</password>
- <sequencing>
- <default-sequence xsi:type="native-sequence">
<name>Native</name>
<preallocation-size>1</preallocation-size>
</default-sequence>
</sequencing>
<driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
```

```
<connection-url>jdbc:oracle:thin:@%hostname%:%port%:%database
sid%</connection-url>
  </login>
- <connection-pools>
- <read-connection-pool>
  <name>ReadConnectionPool</name>
<max-connections>5</max-connections>
<min-connections>5</min-connections>
</read-connection-pool>
- <write-connection-pool>
  <name>default</name>
<max-connections>25</max-connections>
  <min-connections>25</min-connections>
  </write-connection-pool>
  </connection-pools>
<connection-policy />
</session>
</toplink-sessions>
```

JDBC String for RAC Database

The correct connection URL for RAC databases is shown below.

```
<connection-url>jdbc:oracle:thin:@(description = (address = (protocol = tcp)(host
= XXhost1XX)(port = 1521))(address = (protocol = tcp)(host =XXhost2XX)(port =
1521))(load_balance = yes)(connect_data =(server = dedicated)(service_name =
XXservice_nameXX)(failover_mode =(type = select)(method = basic)(retries =
100)(delay = 5)))) </connection-url>
```

Globalization Support for Microsoft SQL Server

To support Globalization with Microsoft SQL Server, please remove the "sendStringasUnicode= false" string from the JDBC URL.

13.2 Configuring sessions.xml for JNDI

To configure sessions.xml for JNDI

1. Copy your `sample_jndi.sessions.xml` reference file into a sessions.xml file. The `sample_jndi.sessions.xml` file is located under the /WEB-INF/classes directory.
2. Modify or add the following tags with the appropriate values. Refer to "sessions.xml Tags for JNDI" for more information.
   - `<platform-class>`
   - `<external-connection-pooling>`
   - `<datasource>`

13.2.1 sessions.xml Tags for JNDI

The tags to modify or add are explained below.

<platform-class>

Modify the <platform-class> tag. Refer to "TopLink platform-class" for the platform specific property that you will modify the TopLink <platform-class> tag with.

<external-connection-pooling>

Modify the <external-connection-pooling> tag. An example in bold type is provided in the "sessions.xml File Sample for JNDI" section.

<datasource>

Modify the <datasource> tag. For example,

```
<datasource>%datasource name%</datasource>
```

> **Note:** For a RAC database, use the RAC JDBC string for the datasource.

For another example, refer to the "sessions.xml File Sample for JNDI" section.

13.2.2 sessions.xml File Sample for JNDI

For your reference, a sessions.xml file is provided below.

```
<?xml version="1.0" encoding="UTF-8"?>
<toplink-sessions version="10g Release 3 (10.1.3.1.0)"
                  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <session xsi:type="server-session">
        <name>default</name>
        <event-listener-classes/>
        <primary-project xsi:type="xml">BharosaTLMappings.xml</primary-project>
        <login xsi:type="database-login">

<platform-class>oracle.toplink.platform.database.oracle.Oracle10Platform</platform
-class>
            <external-connection-pooling>true</external-connection-pooling>
            <sequencing>
                <default-sequence xsi:type="native-sequence">
                    <name>Native</name>
                    <preallocation-size>1</preallocation-size>
                </default-sequence>
            </sequencing>
            <datasource>%oarm_ds%</datasource>
        </login>
        <connection-policy/>
    </session>
</toplink-sessions>
```

13.3 TopLink platform-class

Platform specific property that you modify the TopLink <platform-class> tag with are listed below.

13.3.1 Oracle

Oracle TopLink <platform-class> tag that you will need to modify are listed below.

Oracle - Generic

```
oracle.toplink.platform.database.OraclePlatform
```

Oracle10g (10.1.0.3)

```
oracle.toplink.platform.database.oracle.Oracle10Platform
```

For WebLogic:

```
com.bharosa.common.db.wldbutil.Oracle10PlatformLOBUtil
```

Oracle10g (10.2.0.1)

```
oracle.toplink.platform.database.oracle.Oracle10Platform
```

For WebLogic:

```
com.bharosa.common.db.wldbutil.Oracle10PlatformLOBUtil
```

Note: For WebLogic, use Oracle drivers with the Utility class. The WebLogic database drivers will not work with the Utility class.

13.3.2 Microsoft

SQL Server 2005

```
oracle.toplink.platform.database.SQLServerPlatform
```

14

Setting Up Background Images

The Adaptive Strong Authenticator device uses personalized images to enhance security. Oracle provides you with a compressed file of images.

14.1 Setting Up the Images for Authentication Devices

To modify the authentication devices information

1. Create a background images directory inside a file system that can be accessed by Adaptive Risk Manager Online. Ensure that the directory is secure with restricted access privileges.
2. Uncompress the image archive to that directory.
3. Add the following property to the bharosa_client.properties file.

   ```
   bharosa.image.dirlist=/bharosa_images/allpads/textpad/
   ```

4. Update the bharosa_server.properties file to point to the shared images directory.

   Ensure that you have the path set correctly. If the image path is not configured properly, the images will not display in Adaptive Strong Authenticator.

   Note: Each server machine should have the images, and the property files should have the same path configurations.

14.2 Sample Code

Code sample in bold type is provided below.

```
#this is to point to the shared image directory, both bharosa_client.properties
and bharosa_server.properties
#should point to the same value

bharosa.image.dirlist=/bharosa_images/allpads/textpad/
```

15

Configuring Client Properties

For Adaptive Strong Authenticator (SOAP) and Native Integration (SOAP), the following properties must be configured in the bharosa_client.properties file:

- SOAP URL
- Image path
- Image URL
- Proxy mode
- SOAP class
- Password Used for Testing
- Configuration Value Encryption
- SOAP/Web Services Access
- SOAP Authentication (if it needs to be enabled/disabled)
- Case in Username (Optional)

15.1 Modifying the bharosa_client.properties File

To modify the bharosa_client.properties file

1. Copy sample.bharosa_client.properties to bharosa_client.properties. The sample file is located under the oasa/WEB-INF/classes/ directory.
2. In bharosa_client.properties, update the appropriate property values as described in "Properties".

   Note: A trailing slash will cause an error when deploying Adaptive Strong Authenticator in WebLogic.

3. Back up and secure the bharosa_client.properties file in case you should need to restore any customer specific customizations or upgrade to Adaptive Risk Manager software at a later date.

15.2 Properties

Properties to edit are documented below.

SOAP URL

Set the vcrypt.tracker.soap.url property.

For example,

```
vcrypt.tracker.soap.url=http://localhost:7001/oarm/services/
```

Image Path

Add the bharosa.image.dirlist property.

For example,

```
bharosa.image.dirlist=/bharosa_images/allpads/textpad/
```

Image URL

Set bharosa.authentipad.image.url as follows:

bharosa.authentipad.image.url=kbimage?action=kbimage&

Proxy Mode

Add the bharosa.uio.proxy.mode.flag property and set it to true or false.

When there is no proxy involved, set it to false.

SOAP Class

Set the vcrypt.common.util.vcryptsoap.impl.classname property.

Options are:

com.bharosa.vcrypt.common.impl.VCryptSOAPWeblogicImpl: Uses WebLogic implementation

com.bharosa.vcrypt.common.impl.VCryptSOAPAxisImpl: Uses Apache implementation

Password Used for Testing

Configure the password used for testing in the non-proxy mode. For example,

```
#Set the dummy password for testing in non-proxy mode.
bharosa.uio.login.dummy.password=test
```

Configuration Value Encryption Properties

Ensure that you have the keystore and alias passwords properties set.

```
bharosa.cipher.encryption.algorithm.enum.DESede_config.keystorePassword=<base64
encoded keystore password>
bharosa.cipher.encryption.algorithm.enum.DESede_config.aliasPassword=<based64
encoded password to the alias>
```

The encoded passwords are generated during the creation of system_config.keystore. Refer to Chapter 10, "Setting Up Encryption" for more information.

SOAP/Web Services Access

Ensure that you have the keystore and alias passwords and web service username properties set if you are using Web services.

```
vcrypt.soap.auth.keystorePassword=<base64 encoded keystore password>
vcrypt.soap.auth.aliasPassword=<based64 encoded password to the alias>
vcrypt.soap.auth.username=<user configured for accessing the soap services>
```

```
vcrypt.soap.auth.keystoreFile=system_soap.keystore
```

The encoded passwords are generated during the creation of system_soap.keystore. Refer to Chapter 11, "Configuring SOAP/Web Services Access" for more information.

SOAP Authentication

To disable or enable, HTTP authentication for Adaptive Strong Authenticator, set the following property to true (enabled) or false (disabled).

```
vcrypt.soap.auth=
```

For information about disabling Web Services for Adaptive Strong Authenticator/Native Client, refer to Chapter 11, "Configuring SOAP/Web Services Access."

Case in Username

If you want the username to be in lowercase, set bharosa.uio.default.username.case.sensitive to false.

16

Setting Up Logging

Adaptive Risk Manager enables detailed logging through log4j logging mechanisms.

Log4j options that Adaptive Risk Manager uses are:

- Appenders - Used to define where log output goes. Appenders can output to files, SMTP (email), JDBC (database), or even JMS. Multiple appenders of the same type can be defined.
- Loggers - Used to define to which appenders output is logged. Loggers can have multiple appenders attached to them.

This logging system is configured by placing the log4j.xml file in the web application's WEB-INF/classes folder and by specifying the log output path for appenders and the level of logging.

16.1 Pre-requisites for Email Alerts

For email alerts to work, third-party libraries must be copied into the WEB-INF/lib folder. The required files are

- activation.jar, which can be downloaded from http://java.sun.com/javase/technologies/desktop/javabeans/jaf/index.jsp
- mail.jar, which can be downloaded from http://java.sun.com/products/javamail/

16.2 Create a Log Directory

Create directories for the log files.

Oracle recommends the directory/file permission should be (rw-,r---). Only the install owner and group should be allowed to read these files due to the sensitive nature of the information that could be contained within them.

16.3 Editing the Log4j.xml Parameters

There are various parameters that can be configured in log4j.xml based on application needs.

To edit log4j.xml parameters,

1. Locate the log4j.xml file under the oarm/WEB-INF/classes/ directory.
2. Update the log output path for each appender.

3. Search for <param name="File" value=" and change the file path for the logs appropriately.
4. Configure SMTP for emailing warnings and errors (optionally).

16.4 Commonly Edited log4j.xml Parameters

A list of commonly edited log4j.xml parameters is shown below. If you want your log files to be created in a non-default location, specify the path for the log file location. Refer to the highlighted text below.

```
<appender name="FILE" class="org.apache.log4j.DailyRollingFileAppender">
        <param name="File" value="/home/logs/oarm_log.txt" />
        <param name="DatePattern" value="'.'yyyy-MM-dd-HH" />
        <layout class="org.apache.log4j.PatternLayout">
             <param name="ConversionPattern" value="%d
%-5p[app=%log4j.webapp.name%] [%t] %c - %m\n" />
        </layout>
</appender>
```

Note: Ensure that you have the log file location set correctly.

16.5 Levels of Alert

Output in the logs can be configured for different levels--from detailed to specific data logging--based on the application requirements and space. The set of possible levels include INFO, WARN, ERROR and FATAL.

To change the level of logging, update the value in <level value >. Refer to the example below:

```
<logger name="com.bharosa">
<level value="INFO" />
</logger>

<logger name="AlertEmail" additivity="false">
        <appender-ref ref="ALERT_EMAIL" />
  </logger>
```

Our alerts correspond to the following log4j levels:

- FATAL - for high alerts
- ERROR - for medium alerts
- WARN - for low alerts
- INFO - for details on the alerts

16.6 Fraud Detection

For "instant alert" fraud detection, we recommend setting up an SMTP appender for alerts only. Refer to the example shown below:

```
<appender name="ALERT_EMAIL" class="org.apache.log4j.net.SMTPAppender">
       <param name="BufferSize" value="512" />
       <param name="SMTPHost" value="localhost" />
       <param name="From" value="vadmin" />
       <param name="To" value="lenny@localhost" />
```

```
            <param name="Subject" value="[app=fauio]Log4j:Bharosa" />
            <layout class="org.apache.log4j.PatternLayout">
                 <param name="ConversionPattern"
value="[%d{ISO8601}]%n%n%-5p%n%n%c%n%n%m%n%n" />
            </layout>
        </appender>
```

In order to use this appender, add the logger to the log4j.xml file as shown below:

```
<logger name="AlertEmail" additivity="false">
     <level value="fatal"/>
<appender-ref ref="ALERT_EMAIL" />
  </logger>
```

16.7 Levels of Alert

Output in the logs can be configured for different levels--from detailed to specific data logging--based on the application requirements and space. The set of possible levels include INFO, WARN, ERROR and FATAL.

Our alerts correspond to the following log4j levels:

- FATAL - for high alerts
- ERROR - for medium alerts
- WARN - for low alerts
- INFO - for details on the alerts

16.8 Best Practices

Future patches or releases might overwrite your customizations; ensure that you make a backup copy of the log4j.xml file in the event that a patch is applied to the installation and you need to perform a restore.

17

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.

The languages and their locale identifiers are listed below. A locale identifier consists of at least a language identifier, and a region identifier (if required).

Adaptive Risk Manager is translated into French (fr), German (de), Italian (it), Spanish (es), Brazilian Portuguese (pt_br), Japanese (ja), Korean (ko), Simplified Chinese (zh_cn), and Traditional Chinese (zh_tw).

Adaptive Strong Authenticator is translated into 26 languages: French (fr), German (de), Italian (it), Spanish (es), Brazilian Portuguese (pt_br), Japanese (ja), Korean (ko), Simplified Chinese (zh_cn), Traditional Chinese (zh_tw) Arabic (ar), Czech (cs), Danish (da), Dutch (nl), Finnish (fi), Greek (el), Hebrew (iw), Hungarian (hu), Norwegian (no), Polish (pl), Portuguese (pt), Romanian (ro), Russian (ru), Slovak (sk), Swedish (sv), Thai (th), and Turkish (tr).

This chapter provides information on customizing Oracle Adaptive Access Manager for your locale.

17.1 Configuring Language Defaults for Oracle Adaptive Access Manager

Information about the supported locales for a deployment is declared in a user-defined enum named bharosa.locale.enum in the common_enums.properties file.

In the default deployment configuration, there are bharosa.locale.enums defined for the supported locales. For Adaptive Strong Authenticator, 10 languages are enabled.

An example of a bharosa.locale. enum is shown below.

```
bharosa.locale.enum.german=2
bharosa.locale.enum.german.name=German
bharosa.locale.enum.german.description=German
bharosa.locale.enum.german.language=de
bharosa.locale.enum.german.country=
bharosa.locale.enum.german.adminSupported=true
bharosa.locale.enum.german.enabled=true
```

In the default deployment configuration, there are bharosa.locale.enums defined for the supported locales.

The common_enums.properties file is located in the <webapps_install_directory>/<webapps_name>/WEB-INF/classes directory.

Use this file to look up the exact property names for the desired locales so that you can add, or add and modify the properties in bharosa_server.properties for Adaptive Risk Manager and bharosa_client.properties for Adaptive Strong Authenticator.

Note: Do not edit the common_enums.properties file.

To configure language defaults for Oracle Adaptive Access Manager, you will need to perform Steps 1 and 2 for bharosa_server.properties (for Adaptive Risk Manager) and bharosa_client.properties (for Adaptive Strong Authenticator), and then restart the server for the changes to take effect.

1. Copy the bharosa.local.enum.<locale>.enabled properties of the locales you want to support and ensure they are set to true.
2. Copy the bharosa.local.enum.<locale>.enabled properties of the locales you do not want to support and ensure they are set to false.
3. Copy the bharosa.default.locale property and set its value to match the value of the desired locale's bharosa.locale.enum.<locale> property.

Example configuration scenarios are presented below.

17.1.1 Example 1

A German bank wants to set German as the default language and wants to support only German. To do this:

1. Copy bharosa.locale.enum.german.enabled=true into bharosa_server.properties.
2. Copy all other bharosa.local.enum.<locale>.enabled properties into bharosa_server.properties and ensure they are set to false.
3. Copy the bharosa.default.locale property into bharosa_server.properties and set it to the value of the locale enum.

   Since bharosa.locale.enum.german=2, set bharosa.default.locale property to 2.
4. Copy bharosa.locale.enum.german.enabled=true into bharosa_client.properties.
5. Copy all other bharosa.local.enum.<locale>.enabled properties into bharosa_client.properties and ensure they are set to false.
6. Copy the bharosa.default.locale property into bharosa_client.properties and set it to 2.
7. Restart the server for the changes to take effect.

17.1.2 Example 2

A Swiss bank wants to set German as the default, but wants to display in Adaptive Strong Authenticator in all the other languages that Adaptive Strong Authenticator had been translated to. To do this:

1. Copy bharosa.locale.enum.german.enabled=true into bharosa_server.properties.
2. Copy all other bharosa.local.enum.<locale>.enabled properties into bharosa_server.properties and ensure they are set to false.
3. Copy the bharosa.default.locale property into bharosa_server.properties and set it to the value of the locale enum.

   Since bharosa.locale.enum.german=2, set bharosa.default.locale property to 2.

4. Copy the bharosa.locale.enum.<locale>.enabled property into bharosa_client.properties for all the languages Adaptive Strong Authenticator had been translated to and ensure they are set to true.

```
bharosa.locale.enum.german.enabled=true
bharosa.locale.enum.italian.enabled=true
bharosa.locale.enum.french.enabled=true
bharosa.locale.enum.portuguese_br.enabled=true
bharosa.locale.enum.spanish.enabled=true
bharosa.locale.enum.korean.enabled=true
bharosa.locale.enum.chinese_cn.enabled=true
bharosa.locale.enum.chinese_tw.enabled=true
bharosa.locale.enum.japanese.enabled=true
bharosa.locale.enum.arabic.enabled=true
bharosa.locale.enum.czech.enabled=true
bharosa.locale.enum.danish.enabled=true
bharosa.locale.enum.dutch.enabled=true
bharosa.locale.enum.finnish.enabled=true
bharosa.locale.enum.greek.enabled=true
bharosa.locale.enum.hebrew.enabled=true
bharosa.locale.enum.hungarian.enabled=true
bharosa.locale.enum.norwegian.enabled=true
bharosa.locale.enum.polish.enabled=true
bharosa.locale.enum.portuguese.enabled=true
bharosa.locale.enum.romanian.enabled=true
bharosa.locale.enum.russian.enabled=true
bharosa.locale.enum.slovak.enabled=true
bharosa.locale.enum.swedish.enabled=true
bharosa.locale.enum.thai.enabled=true
bharosa.locale.enum.turkish.enabled=true
```

5. Copy the bharosa.default.locale property into bharosa_client.properties and set the value to 2.
6. Restart the server for the changes to take effect.

17.1.3 Example 3

A French bank wants clients to see French as a default, and wants to support only French, German, English, and Italian. To do this:

1. Copy the bharosa.locale.enum.<locale>.enabled properties into bharosa_server.properties for French, German, Italian, and English and ensure they are set to true.

```
bharosa.locale.enum.french.enabled=true
bharosa.locale.enum.german.enabled=true
bharosa.locale.enum.italian.enabled=true
bharosa.locale.enum.english.enabled=true
```

2. Copy all other bharosa.local.enum.<locale>.enabled properties into bharosa_server.properties and ensure they are set to false.
3. Copy bharosa.default.locale property into bharosa_server.properties and set it to the value of the locale enum.

   Since bharosa.locale.enum.french=5, set bharosa.default.locale property to 5.

4. Copy the bharosa.locale.enum.<locale>.enabled properties into bharosa_client.properties for French, German, and Italian and ensure they are set to true.
5. Copy all other bharosa.local.enum.<locale>.enabled properties into bharosa_client.properties and ensure they are set to false.
6. Copy bharosa.default.locale property into bharosa_client.properties and set it to 5.
7. Restart the server for the changes to take effect.

17.2 Adding to the Abbreviation File

Oracle Adaptive Access Manager supports the concept of "fuzzy logic." Fuzzy logic, in part, relies on pre-configured sets of word equivalents, commonly known as abbreviations.

In the English version of Oracle Adaptive Access Manager, there are several thousand English abbreviations (and equivalences). In all other languages, it is necessary for the installer to enhance the brief abbreviation files provided. Without additions to the file, the fuzzy logic will be not as effective.

To add abbreviations:

1. Open the bharosa_auth_abbreviation_config_<locale>.properties file. The file is located in the <webapps_install_directory>/<webapps_name>/WEB-INF/classes directory.
2. Add as many abbreviations and equivalences as you want.

   There are two different formats you can use:

   ```
   Word=equivalent1
   Word=equivalent2
   ```

   or

   ```
   Word=equivalent1,equivalent2, equivalent3
   ```

   For example, in English you can add some of the equivalence for James:

   ```
   Jim=James,\Jamie,\Jimmy
   ```

   With the addition of the equivalences, if a client were to enter a response as Jim, but had originally entered James, Jim would be accepted.

   Another example is that "St" may be equivalent to Street.
3. Restart the server for the changes to take effect.

> **Note:** Retrieval of abbreviation values is not based on the browser language; values are retrieved from all the bharosa_auth_abbreviation_config_<locale>.properties files.

17.3 Adding Registration Questions

During registration, Oracle Adaptive Access Manager presents customers with three question menus. When a customer registers, he or she is required to select one question from each menu. These three questions become the customer's "registered questions."

To add questions in Oracle Adaptive Access Manager:

1. Log in to Adaptive Risk Manager
2. On the Admin menu, point to KBA, point to Questions, and then click Create New Question.
3. Pick a locale from the list of locales available.
4. Type the new question in the Question field.

> **Note:** The deployment administrator must ensure there are enough questions in the database for each of the supported locale as configured in Adaptive Risk Manager during deployment; otherwise, Adaptive Strong Authenticator displays only the English language questions during registration. The number of locale-specific questions must be equal to or greater than the "Questions Per Menu" * "Categories Per Menu" * "Questions User Will Register".

Refer to "KBA Challenge Questions" in the *Oracle Adaptive Access Manager Administrator's Guide*.

17.4 Configuring Words Used in the Authenticator Caption

During initial registration a user is assigned a word:word pair for their keypad that is generated randomly from word list properties. In English the word:word pairs are in the form, adjective:noun.

In the English version of Oracle Adaptive Access Manager, there are several hundred values in the word lists. In all other languages it is necessary for the installer to enhance the brief word lists provided.

To add words to the word lists:

1. Open the authentipad_msg_resource_<locale>.properties file. The file is located in the <webapps_install_directory>/<webapps_name >/WEB-INF/classes directory.
2. Modify the bharosa.user.caption.word1.list and bharosa.user.caption.word2.list properties.
3. Restart the server for the changes to take effect.

17.5 Configuring "Enter" on the Authenticator Forgot Password Page

A bank wants clients to see "Enter" in its own language on the TextPad's Forgot Password page. To do this:

1. Open the authentipad_msg_resource_<locale>.properties file. The file is located in the <webapps_install_directory>/<webapps_name >/WEB-INF/classes directory.
2. Modify the bharosa.uio.default.forgotpassword.primary.page.message= property.
3. Restart the server for the change to take effect.

17.6 Configuring Tooltip for TextPad's "Enter" Button

A bank wants clients to see "Enter" in its own language for the TextPad's tooltip. To do this:

1. Open the authentipad_resource_<locale>.properties file. The file is located in the <webapps_install_directory>/<webapps_name >/WEB-INF/classes directory.
2. Modify the bharosa.authentipad.textpad.enterkey.label=enter property.
3. Restart the server for the change to take effect.

18

BI Publisher Reports

Oracle Identity Management Business Intelligence (BI) Publisher Reports enables you to use Oracle BI Publisher as the reporting solution for Oracle Identity Management products including Oracle Adaptive Access Manager.

This chapter provides information installing Oracle Adaptive Access Manager BI Publisher Reports.

18.1 Prerequisites

To install the Oracle Adaptive Access Manager BI Publisher Reports you must have working versions of the following:

- BI Publisher 10.1.3.4.0 or higher. For information on the installation of BI Publisher, refer to the *Oracle Business Intelligence Publisher Installation Guide*.
- Adaptive Risk Manager 10.1.4.5.0 or higher.

18.2 Installation

This chapter provides instructions to install the Oracle Adaptive Access Manager BI Publisher Reports and contains the following sections:

18.2.1 Unzip oaam_bipreports_oradb.zip

The oaam_bipreports_oradb.zip file contains the Oracle Adaptive Access Manager reports. Unzip it in the oaam_reports directory.

18.2.2 Stop the BI Publisher Server

Instructions to stop the BI Publisher server is given in the BI_Publisher_Readme.txt file located in the <BI Publisher Oracle Home> directory. If you had installed BI Publisher using the Basic Install, the syntax to stop the Oracle BI Publisher is as follows:

```
<Java 1.5 Home>/bin/java.exe -jar <BI Publisher Oracle Home>/oc4j_
bi/j2ee/home/admin.jar ormi://<host>:<port>  oc4jadmin <oc4jadmin password>
-shutdown for
```

For example,

```
/BIPOraHome/jdk/bin/java.exe -jar /BIPOraHome/oc4j_bi/j2ee/home/admin.jar
ormi://idmbip:23791 oc4jadmin oc4jadmin -shutdown force
```

18.2.3 Copy the Oracle Adaptive Access Manager Report Files

Copy the entire folder, which contains the reports, to the <BI Publisher Oracle Home>/XMLP directory in the Oracle BI Publisher server's file system.

18.2.4 Copy properties.xml to the Oracle BI Publisher Server's File System

Copy the properties.xml file to any directory in Oracle BI Publisher server's file system.

18.2.5 Start the BI Publisher Server

Instructions to start the BI Publisher server is given in the BI_Publisher_Readme.txt file located in the <BI Publisher Oracle Home> directory. If you had installed BI Publisher using the Basic Install, the syntax to start the Oracle BI Publisher is as follows:

```
<BI Publisher Oracle Home>/oc4j_bi/bin/oc4j.cmd -start
```

Example:

```
/BIPOraHome/oc4j_bi/bin/oc4j.cmd -start
```

18.2.6 Configure JDBC Data Source

To configure the JDBC data source:

1. Login to the Oracle BI Publisher as an administrator.

   The URL is http://<ip address>:8080/xmlpserver/

2. Click the Admin tab.
3. In the Data Source section, click JDBC Connection.
4. Click Add Data Source to add a new JDBC type data source to access the Oracle Adaptive Access Manager database.
5. Fill in the Add Data Source form.

   Data Source Name: ARM

   Connection String: jdbc:oracle:thin:@<host>:<port>:<sid>

   User Name: <database username>

   Password: <database password>

Database Driver Class: oracle.jdbc.driver.OracleDriver

For example:

Data Source Name: ARM

Connection String: jdbc:oracle:thin:@oaam:1521:brsadb

User Name: oaamdbuser

Password: abcd1234

Database Driver Class: oracle.jdbc.driver.OracleDriver

Note: For the Oracle Adaptive Access Manager reports to work out-of-the-box, the JDBC data source must be named as "ARM". If you choose a different name, you will need to modify the data source property in all reports.

18.2.7 Configure AdminProperties Data Source

To configure the AdminProperties data source:

1. Click the Admin tab.
2. In the Data Source section, click File.
3. Click Add Data Source.
4. Fill in the Add Data Source form.

   Data source name must be "AdminProperties"

   Path must be the directory where we placed properties.xml

18.2.8 Test the Reports

To test the reports:

1. Login to Oracle BI Publisher as an administrator, and then click Shared Folders.

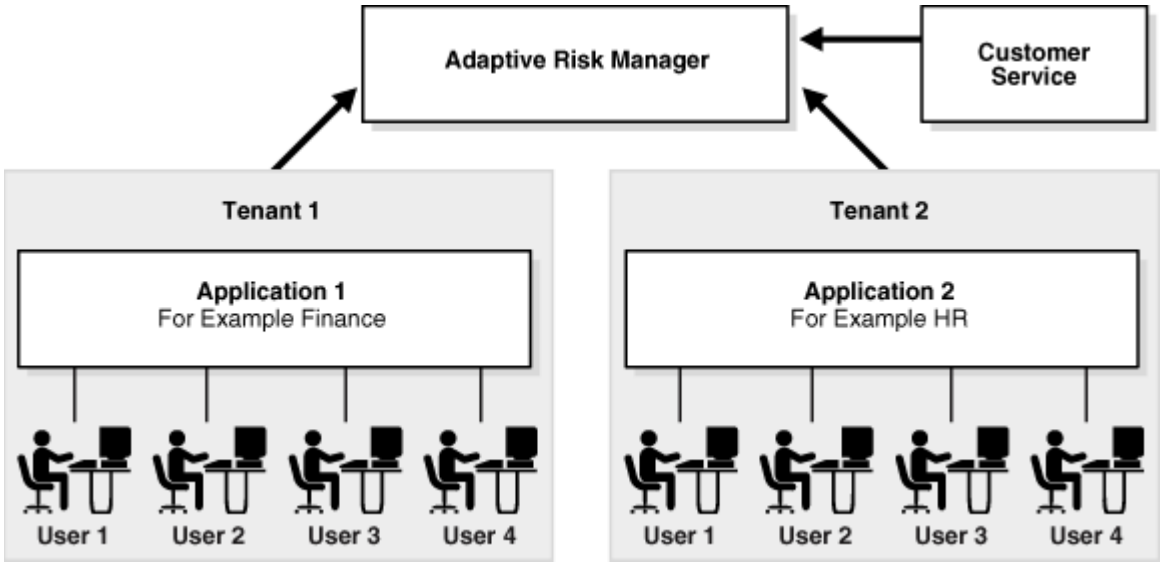
   You will see a new folder, "OAAM Reports," on the "Shared Folders" page.
2. Click "oracle" under "OAAM Reports."
3. Choose any report.
4. Choose any output type and click the View button.

19

Multi-Tenant Support

Oracle Adaptive Access Manager by default is enabled for multitenancy. A single instance of Oracle Adaptive Access Manager can support multiple client applications. Models and Rules can be centrally administrated and can be shared between applications, with the option to personalize for individual applications. Customer Care Admin users can be restricted to create and view cases only for users from their applications. Adaptive Strong Authenticator can also be personalized for each application for look and feel.

Figure 19–1 Multi-Tenant Scenario Example



19.1 Configuring Access Control for Customer Care Uses

In the bharosa_server.properties file, please update the following properties:

```
#This enables check for access control for CSR users in ARM

bharosa.multitenant.enforce.admin.check=true

#List the admin roles have super user roles. Users with this role will have access
to all the users with OAAM. You can provide multiple roles separated by comma

bharosa.multitenant.superuser.ldap_groups=
```

For each application (tenant), create an Oracle Adaptive Access Manager User Defined Enum element. An example of the properties is shown below.

```
#Replace Tenant1, Tenant2, ... with your appIds
bharosa.extgroupid.enum.Tenant1=2
bharosa.extgroupid.enum.Tenant1.name=Tenant1
bharosa.extgroupid.enum.Tenant1.description=Tenant one group
#List the roles (separated by comma) who have access to this Tenant.
bharosa.extgroupid.enum.Tenant1.ldap_groups=Tenant1
#If this is true, then access control will be enforced for this tenant.
bharosa.extgroupid.enum.Tenant1.access_control_adminusers=true

bharosa.extgroupid.enum.Tenant2=3
bharosa.extgroupid.enum.Tenant2.name=Tenant2
bharosa.extgroupid.enum.Tenant2.description=Tenant two group
bharosa.extgroupid.enum.Tenant2.ldap_groups=Tenant2
bharosa.extgroupid.enum.Tenant2.access_control_adminusers=true
```

20

What to Do Next

After the installation and configuration of the Oracle Adaptive Access Manager components, you can log in to the web application and start using it.

20.1 Starting the Database and Application Server

Before you can access the application, you must

1. Ensure that the database server, where the Oracle Adaptive Access Manager repository schema was created, is up and running.
2. Start the application server.

20.2 Logging in to Adaptive Risk Manager Online

To log in to Adaptive Risk Manager Online, enter the following URL:

http or https://<ip address>:<port>/oarm

It is http by default.

When you are prompted, enter a username and password of one of the users you created in Section 6.1, "Creating Groups/Roles."

20.3 Logging in to Adaptive Risk Manager Offline

To log in to Adaptive Risk Manager Offline, enter the following URL:

http or https://<ip address>:<port>/oarm_offline

It is http by default.

When you are prompted, enter a username and password of one of the users you created in Section 6.1, "Creating Groups/Roles."

20.4 Logging in to Adaptive Strong Authenticator

To log in to Adaptive Strong Authenticator, enter the following URL:

http or https://<ip address>:<port>/oasa

It is http by default.

When you are prompted, enter a username and the password, "test."

Note: Oracle Adaptive Access Manager supports passwords in 9 admin languages minus CJK characters.

20.5 Using Adaptive Access Manager

Perform some or all of the steps listed below to enable the features you will be using.

1. Import the up-to-date base security and business models into Adaptive Risk Manager.

   On the Admin menu, point to Models, then click Import Models.

2. Import auth entities (Auth_EntityDefinition.zip) into Adaptive Risk Manager. Auth entities are the default entities that are required for the operation of the Auto-learning feature. Auto-learning data collection and rules will not run properly without the them.

   On the Admin menu, point to Entities, then click Import Entities.

3. Import the full package of rule conditions (oaam_rule_conditions/oaam_rule_conditions.zip) into Adaptive Risk Manager.

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

   For a list of these conditions, see the *Oracle Adaptive Access Manager Administrator's Guide*.

4. Import all challenge questions from the oaam_kba_questions_<locale>.zip file, which is available in the release package. The questions must be imported for successful registration and login in Adaptive Strong Authenticator.

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

5. Enable phase 2 scenarios by adding default user group to Phase 2 pre- and post-authentication business models.

   Phase 2 provides optional registration scenarios that you may want to try out with users. If you find that the users like to use the registration process, you may add the scenarios to your authorization process.

   To enable Phase 2 scenarios

   a. Ensure that "Active" has been chosen for the status of the model.

   b. Ensure that all the rules in the model are active.

   c. Ensure that "All Users" has been selected for the Run Mode option.

      For versions of Oracle Adaptive Access Manager prior to 10.1.4.5, you must explicitly link users using the Group Linking tab in the Model Details page.

Using Oracle Adaptive Access Manager, you can create your own models, rules, and challenge questions. For step-by-step instructions, see the *Oracle Adaptive Access Manager Administrator's Guide*.

21

Troubleshooting Adaptive Risk Manager

This chapter describes common troubleshooting issues and tips to resolve them. The following topics are covered:

21.1 Oracle Adaptive Access Manager is Slow to Respond

Oracle Adaptive Access Manager is slow to respond; and diagnostics, logs, and errors--such as "hogging thread counts and a large number of SQL*net and RX errors--indicate a network issue.

If you are experiencing a network performance issue, monitor your network interface using a network utility like Ethtool (for Linux) to help you analyze your network bottleneck.

21.2 Initialization Parameters Do Not Change When Altering

Problem: When initialization parameters were altered with the `alter system set <PARA>=<VALUE> scope=spfile` command as per the instructions in the "Oracle Initialization Parameters" section, the values did not appear to change.

Solution: Restart the database.

21.3 Tables Are Not Built After Running db_setup.sql

Problem: The tables were not created after running the db_setup.sql script. An error message appears, stating that the table or view does not exist.

Solution: The user created did not have the right file permissions; therefore, the tablespace could not be created. Ensure that the user has the right file permissions.

21.4 Jar Command Not Found

Ensure that the JAVA_HOME environment variable is set to point to the Java installation directory. For example /usr/java.

Also check that the CLASSPATH or PATH environment variable is defined and has the Java core libraries listed (among other items). For example, CLASSPATH=/usr/java/lib/.

21.5 Background Images Are Not Displayed in Adaptive Strong Authenticator

Check the background images path configured in bharosa_client.properties.

21.6 Log4j

Note that asynchronous appenders are not recommended in the log4j configuration.

Make sure directories referenced in all appender sections are physically present and accessible to the application server. In the example configurations below, make sure "/logs/" & "/home/abc/toplink/" directory mentioned below is present and accessible.

Example:

```
<appender name="BHAROSA_FILE" class="org.apache.log4j.DailyRollingFileAppender">
     <param name="File" value="/logs/bharosauio_bharosa_log.txt"/>
     <param name="DatePattern" value="'.'yyyy-MM-dd-HH"/>
     <layout class="org.apache.log4j.PatternLayout">
         <param name="ConversionPattern" value="%d %-5p [app=bharosauio] [%t] %c -
%m\n"/>
```

```
     </layout>
 </appender>
<appender name="TOPLINK_FILE" class="org.apache.log4j.DailyRollingFileAppender">
    <param name="File" value="/home/abc/toplink/bharosauio_toplink_log.txt"/>
    <param name="DatePattern" value="'.'yyyy-MM-dd-HH"/>
    <layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%d %-5p [app=bharosauio] [%t] %c -
%m\n"/>
    </layout>
</appender>
```

21.7 SOAP Service Calls Throws Exceptions

Check if the remote calls do have DNS lookup or network connectivity. Check the DNS lookup capabilities. Using IP, instead of name may be faster.

Make sure soap time out is not set to too low. Parameter "vcrypt.soap.call.timeout" affects the timeout and default is set to 3000 (3 secs)

21.8 Adaptive Risk Manager Online Is Not Accessible

Check the port on which the application server is active and serving the Adaptive Risk Manager Online application.

Make sure DNS entry is correct and/or IP Address is accessible.

21.9 Rule Execution Logs Do Not Appear In Session Details

Rule execution logs are written asynchronously and may not be available immediately. Check back later to see if they are available.

21.10 Unable to Login Into Adaptive Risk Manager

Check that the user id has access and is a member of the predefined roles. The roles are defined in the application server for Adaptive Risk Manager.

21.11 Adaptive Risk Manager Online Is Accessible But Queries Return Database Errors

Ensure correct database access credentials are used in the sessions.xml. If data source is used, make sure data source is configured correctly.

Check that the TCP/IP port specified on the database server for database access is correct and the database server is listening on the port.

21.12 Adaptive Risk Manager Online Application Throws Timeout Errors

Check the timeout settings for the application server container.

21.13 Unable To See All The Menus In Adaptive Risk Manager Online

Check that the user ID is a member of the predefined roles, which were defined in the application server for Adaptive Risk Manager.

21.14 Import Fails in Adaptive Risk Manager Deployed in WebLogic

Problem: Adaptive Risk Manager is deployed in WebLogic server. Import fails with the following error:

```
weblogic.jdbc.wrapper.Clob_weblogic_jdbc_base_BaseClob cannot be cast to
oracle.sql.CLOB
```

Solution: There is a known issue with WebLogic JNDI for handling CLOB. The current recommended workaround is to change the platform class in sessions.xml file to the one provided in the Adaptive Risk Manager distribution. Please refer to Section 13.3.1, "Oracle" in Chapter 13, "Configuring Database Connectivity."

21.15 Rule Conditions Import Causes weblogic.jdbc.wrapper.Clob_ oracle_sql_CLOB Exception

Problem: While importing the rule conditions using Oracle XE configured through JNDI, a weblogic.jdbc.wrapper.Clob_oracle_sql_CLOB exception occurs. The trace references Oracle8Platform.writeLOB.

Solution: Change the platform class in sessions.xml file to com.bharosa.common.db.wldbutil.Oracle10PlatformLOBUtil and restart WebLogic.

21.16 Unable To Reset All User Information From Adaptive Risk Manager Online Customer Care

Check that the user id accessing Adaptive Risk Manager Online customer care is a member of the predefined roles, which were defined in the application server for Adaptive Risk Manager. Refer to Appendix A, "Adaptive Risk Manager User Groups" for more information about roles.

21.17 The Adaptive Risk Manager Online Sample Webapp Deployed To Latest WebSphere 6.1 Throws An Error

The following error message appears:

```
The EAR file might be corrupt or incomplete.
org.eclipse.jst.j2ee.commonarchivecore.internal.exception.DeploymentDescriptorLoad
Exception: WEB-INF/web.xml
```

Solution 1

The error is due to J2EE spec. backward compatibility from IBM WebSphere as noted here - http://www-1.ibm.com/support/docview.wss?uid=swg24009603

The following lines from web.xml needs to be changed:

Old snippet:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE web-app
      PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
     "http://java.sun.com/dtds/web-app_2_3.dtd">
```

*New snippe*t:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.2//EN"
"http://java.sun.com/j2ee/dtds/web-app_2_2.dtd">
```

Solution 2

The error is caused by:
org.eclipse.jst.j2ee.commonarchivecore.internal.exception.DeploymentDescriptorLoad Exception: META-INF/application.xml

Make sure the Web Archive (war) is correctly deployed as an EAR file. It's recommended to deploy using the WAS Admin Console.

21.18 SunJCE Error

Error Message: com.sun.crypto.provider.SunJCE

Error Code: 500

Target Servlet: action

Error Stack:

```
java.lang.NoClassDefFoundError: com.sun.crypto.provider.SunJCE
     at java.lang.J9VMInternals.verifyImpl(Native Method)
```

Make sure the CLASSPATH has jce.jar included. You may need to change the JAVA_HOME to point to non-default Java (default is from IBM which doesn't contain JCE jars). Set `bharosa.security.provider.use.default=true` in `bharosa_server.properties`.

References:

ftp://ftp.software.ibm.com/software/webserver/appserv/library/v61/wasv610base_i_devdep.pdf

http://www-306.ibm.com/software/webservers/appserv/was/library/

21.19 Adaptive Risk Manager Offline Application Server Fails with OutOfMemory Error During Data Load

The Adaptive Risk Manager Offline application server fails with an OutOfMemory error during data load; the environment uses a SQL Server database.

To load login data from a SQL Server database, the JDBC connection string should be updated to include "selectMethod=cursor".

1. On the Admin menu, point to DB Configurations and then click List Configurations.
2. In the Properties tab of your DB Configuration, update "Remote RA DB JDBC URL" to include "selectMethod=cursor", as shown in the example below:

   ```
   jdbc:sqlserver://localhost:1433;databaseName=oaam_offline;selectMethod=cursor
   ```

21.20 Encounter Errors While Trying To Connect To Oracle Database

If you are getting errors while trying to connect to your Oracle database, check the tns listener status.

If the tns listener is not running, start it by issuing the command:

```
lsnrctl start
```

21.21 Operating System Becomes Unresponsive

If the operating system becomes unresponsive while Oracle Adaptive Access

Manager is running under heavy load, please try increasing the "pending signals" value.

The thumb rule is pending signals should be equal to max user processes. By default pending signals is 1024.

```
::ulimit -a::
pending signals (-i) 73728
max user processes (-u) 73728
```

The above can be changed by modifying /etc/security/limits.conf with the following entries:

```
::/etc/security/limits.conf::
aime1        soft     sigpending        73728
aime1        hard     sigpending        73728
```

Note:

1. Oracle Adaptive Access Manager need not be restarted for this change to be effective.
2. This change is applicable to OEL and RHEL.

22

Troubleshooting Adaptive Strong Authenticator

This chapter describes common troubleshooting issues and tips to resolve them. The following topics are covered:

22.1 Server, URL, and Port Problems

A large majority of potential problems related to the Adaptive Risk Manager Online system are due to incorrect settings within client-specific properties files.

When troubleshooting a problem relating to an Adaptive Risk Manager Online installation, ensure that the following two general problems have been addressed:

- Check that the port settings are correct.
- Check the URL to the Web services.

22.2 Adaptive Strong Authenticator Key Pad Troubleshooting

KeyPad does not display.

- Check the property:

  ```
  bharosa.authentipad.image.url=kbimage?action=kbimage&
  ```

- Make certain that the client application is pointing to the correct server application.

Buttons stop jittering.

- Someone has changed the keypad settings. Check with your server personnel regarding property modifications they may have made.

Same image displayed to all users.

- Check the properties file to make sure that the backgrounds directory setting is correct.

No image displayed in pad background.

- User may have images disabled in the browser.
- Users image may have been deleted from the backgrounds directory.
- Check the properties file to make sure that the backgrounds directory setting is correct.
- Check that Adaptive Risk Manager Online is configured to assign images for personalization.

22.3 Change Password Feature Does Not Work

Oracle Adaptive Access Manager must be integrated with another application in order for the change password feature to work, as Oracle Adaptive Access Manager does not store user passwords. For this reason, when change password is attempted in standalone "test" mode there is no password to update.

22.4 Authorization Failure for SOAP Request by Adaptive Strong Authenticator

If you are unable to access Adaptive Strong Authenticator and an "Authorization Failure" error appears in your client log file, refer to Chapter 11, "Configuring SOAP/Web Services Access" for information on setting up SOAP/Web services access.

A

Adaptive Risk Manager User Groups

The Adaptive Risk Manager users groups can access functionality in Adaptive Risk Manager based on the roles they are assigned. The main user groups are listed as:

- CSRGroup
- CSRManagerGroup
- CSRInvestigator
- Investigator
- InvestigationManager
- RuleAdministratorsGroup
- EnvAdminGroup
- SOAPServicesGroup

The roles are used to set up user roles and groups in the Application Server container. This section summarizes the main user groups, their roles, functionality and level of access in Adaptive Risk Manager.

A.1 Group #1 - CSR

Group #1 has very limited access to Adaptive Risk Manager.

Employee User Group	Employee Members	Group has access to these areas of Adaptive Risk Manager	Notes
Group #1	CSR	Group #1 has very limited access to Adaptive Risk Manager. **Security Dashboard** - No Access **Dashboard**- No access **Queries**- No access **Admin**- No access	username: csr1; password: bharosa123

Employee User Group	Employee Members	Group has access to these areas of Adaptive Risk Manager	Notes
		Cases- CSRs have access to search, open and create CSR type cases. There are no outward facing hyperlinks in any of the screens CSRs have access to. Access to a limited list of actions. No access to bulk edit functions on search cases screen.	1. Add Note 2. Customer Resets a. Image and Phrase 3. Challenge Questions a. Reset Questions b. Reset Question Set c. Unlock Customer d. Ask Question New Features 1. CSR cases - Status "open" - Search & open 2. closed status cases - No access 3. Expired status cases - Search Access 4. Expired status cases - No access to open 5. Change Auth Type - Full Access
		Environment- No access	
		Help - Full access	
		Logout- Full access	

A.2 Group #2 - CSR Manager

Groups #2 members will have the access privileges of Group #1 plus some other limited functionality elsewhere.

Employee User Group	Employee Members	Group has access to these areas of Adaptive Risk Manager	Notes
Group #2	CSR Manager	Groups #2 members will have the access privileges of Group #1 plus some other limited functionality elsewhere.	username: csrm1; password: bharosa123
		Security Dashboard - No Access	
		Dashboard- No access	
		Queries- No location based queries are allowed for Group #2 users. See list of recommended queries below.	Below is a list of queries available to group#2.
		Queries / User	
		Recent Logins	
		Multiple Devices	
		First Login	

Employee User Group	Employee Members	Group has access to these areas of Adaptive Risk Manager	Notes
		Frequent Logins	
		Multiple Failures	
		Queries / Device	
		Recent Logins	
		New Devices	
		Devices by User	
		Multiple Successful Logins	
		Users by Device	
		Multiple Failures	
		Multiple Users	
		Frequent Logins	
		Queries / Summary	
		Full Access	
		Queries / Security	
		Full Access	
		KBA	
		Full Access	
		Admin- No Access	

Employee User Group	Employee Members	Group has access to these areas of Adaptive Risk Manager	Notes
		Cases- No create agent type cases. Hide actions, log and linked/related tabs in agent cases	**1.** Add Note a. New b. Pending c. Closed **2.** Change Status a. New b. Pending c. Closed **3.** Change Severity a. Low b. Medium c. High **4.** Temporary Allow a. Single login b. 2hrs c. Set End Date **5.** Cancel **6.** Customer Resets a. Image b. Phrase c. Image & Phrase d. Customer (All) **7.** Challenge Questions a. Unlock Customer b. Reset Questions c. Reset Question Set d. Next Question e. Ask Question New Features **1.** CSR cases - Status "open" - Search & open Access **2.** Closed status cases - Search & open Access **3.** Expired status cases - Search & Open Access **4.** Agent cases - Search access **5.** Agent cases - No access to open **6.** Escalate a CSR case to Agent case - Full Access **7.** Link Sessions tab in agent cases with escalated status
		Environment- No access	

Employee User Group	Employee Members	Group has access to these areas of Adaptive Risk Manager	Notes
		Help - Full access	
		Logout- Full access	

A.3 Group #3 - CSR Investigator and Investigator

CSR Investigators and Investigators have wide access to Adaptive Risk Manager.

Employee User Group	Employee Members	Group has access to these areas of Adaptive Risk Manager	Notes
Group #3	CSR Investigator and Investigator	CSR Investigators and Investigators have wide access to Adaptive Risk Manager.	username: csri1; password: bharosa123
		Dashboard- Full access	
		Security Dashboard - Full Access	
		Queries- Full access	
		Admin- Read-only	
		Cases- Full access.	No access to bulk editing of cases New Features 1. Open & Closed status CSR cases - Search & open Access 2. Open & Closed status Agent cases - Search & open Access 3. Expired status cases - Search & Open Access 4. Overdue cases - Search & Open Access 5. Escalate a CSR case to Agent case - Full Access 6. Extend the expiration date of cases
		Environment- No access	
		Help - Full access	
		Logout- Full access	

A.4 Group #4 - Investigation Manager

Investigation Managers have wide access to Adaptive Risk Manager.

Employee User Group	Employee Members	Group has access to these areas of Adaptive Risk Manager	Notes
Group #4	Investigation Manager	Investigation Managers have wide access to Adaptive Risk Manager.	username: investm1; password: bharosa123
		Security Dashboard - Full access	
		Dashboard- Full access	

Employee User Group	Employee Members	Group has access to these areas of Adaptive Risk Manager	Notes
		Queries- Full access	
		Admin- Read-only	
		Cases- Full access.	Full access to bulk editing of cases. New Features 1. Open & Closed status CSR cases - Search & open Access 2. Open & Closed status Agent cases - Search & open Access 3. Expired status cases - Search & Open Access 4. Overdue cases - Search & Open Access 5. Escalate a CSR case to Agent case - Full Access 6. Extend the expiration date of cases - Full Access
		Environment- No access	
		Help - Full access	
		Logout- Full access	

A.5 Group #5 - Rule Administrator

Rule Admins have wide access to Adaptive Risk Manager.

Employee User Group	Employee Members	Group has access to these areas of Adaptive Risk Manager	Notes
Group #5	Rule Administrator	Rule Admins have wide access to Adaptive Risk Manager.	username: ruleAdmin1; password: bharosa123
		Security Dashboard - Full Access	
		Dashboard- Full access	
		Queries- Full access	
		Admin- Full access	
		Cases- No access.	
		Environment- No access	
		Help - Full access	
		Logout- Full access	

A.6 Group #6 - Environment Administrator

Limited access to Adaptive Risk Manager. The group is responsible for system/environment administration duties.

Employee User Group	Employee Members	Group has access to these areas of Adaptive Risk Manager	Notes
Groups #6	Env Admin	Limited access to Adaptive Risk Manager to manage the server environment. The server environment includes logging, properties, and enumerations. **Security Dashboard** - No access **Dashboard**- No access **Queries**- No access **Admin**- No access **Cases**- No access **Environment**- Full access **Help** - Full access **Logout**- Full access	username: envAdmin1; password: bharosa123

A.7 Group #7 - SOAP Services

The SOAP user is the credentials used to securely communicate between Adaptive Risk Manager and Adaptive Strong Authenticator (or native API).

Employee User Group	Employee Members	Group has access to these areas of Adaptive Risk Manager	Notes
Groups #7	SOAP user	Access to Adaptive Risk Manager Web services only.	username: envAdmin1; password: bharosa123

B

Upgrading from 10.1.4.3 to 10.1.4.5

This appendix contains information about upgrading the Oracle Adaptive Access Manager application and database repository from 10.1.4.3 to 10.1.4.5.

Note: To configuring encryption, please contact Oracle Support.

If you are upgrading the Oracle Adaptive Access Manager application and database repository from 3.5 to 10.1.4.5, there are two steps involved:

1. Upgrade from 3.5 to 10.1.4.3.
2. Upgrade from 10.1.4.3 to 10.1.4.5

This appendix covers information to upgrade from 10.1.4.3 to 10.1.4.5. For information on upgrading from 3.5 to 10.1.4.3, please refer to Appendix C, "Upgrading from 3.5 to 10.1.4.3."

B.1 Upgrading the Oracle Adaptive Access Manager Application Layer

To upgrade the Oracle Adaptive Access Manager application, please perform the procedures documented below.

This section contains the following topics:

- Export Existing Models
- Shut Down and Clean Up Logs
- Back Up the Existing Web Applications
- Deploy and Configure the Web Applications

B.1.1 Export Existing Models

Before performing the upgrade process, export your existing models. Refer to "Rules and Models" in the *Oracle Adaptive Access Manager Administrator's Guide* for information.

B.1.2 Shut Down and Clean Up Logs

1. Shut down Oracle Adaptive Access Manager-related web applications.
2. Clean up all the old logs.

B.1.3 Back Up the Existing Web Applications

1. For both Adaptive Strong Authenticator and Adaptive Risk Manager, back up all the properties files under the <WEBAPPS_INSTALLED_DIR>/<WEBAPPS_NAME>/WEB-INF/classes directory to an <UPGRADE_TEMP_DIR> directory.

   The properties files will be used later in the upgrade process. An example of backing up the files is shown below.

   ```
   Mkdir c:\upgrade_10g_temp
   Copy  c:\tomcat\webapp\oarm\WEB-INF\classes c:\upgrade_10g_temp\oarm\classes
   Mkdir c:\upgrade_10g_temp\oarm
   Mkdir c:\upgrade_10g_temp\oarm\classes
   ```

   Note: Ensure that this step is performed because certain property files must be copied back into their respective directories once the new war files have been exploded or unjarred.

2. Back up Oracle Adaptive Access Manager (the deployed application) if you want to upgrade the Oracle Adaptive Access Manager components listed below.

   - Adaptive Strong Authenticator (Authenticator)
   - Adaptive Risk Manager (Tracker)

   You could back up Oracle Adaptive Access Manager applications by moving the files to a different directory.

   Note: This is an important step if you should need to restore an old application or any customer specific customizations.

B.1.4 Deploy and Configure the Web Applications

To deploy and configure the web applications:

1. Copy and explode or unjar the new 10.1.4.5 war files (oasa.war and oarm.war) in the webapps directory. These war files are provided with the upgrade patch.
2. Deploy the web applications.

   Please follow your platform-specific vendor-supplied deployment guide for instructions on how to install web applications.

3. Once your web application is deployed, copy the properties files you saved (during Step 1 of the "Back Up the Existing Web Applications" section) into their respective WEB-INF\classes directories.

   For the OASA directory (For example, <ASA_HOME>\WEB-INF\classes)

   - bharosa_client.properties
   - bharosa_app.properties
   - log4j.xml

   For the OARM directory (For example, <ARM_HOME>\WEB-INF\classes)

   - bharosa_server.properties
   - bharosa_app.properties

- log4j.xml
- sessions.xml

B.2 Upgrading the Oracle Adaptive Access Manager Database Repository

The Oracle Adaptive Access Manager database repository needs to be upgraded as part of the Oracle Adaptive Access Manager upgrade process; the Oracle Adaptive Access Manager database is not backwards-compatible. Ensure that you upgrade the Oracle Adaptive Access Manager repository before starting the newly deployed application; otherwise, there will be exceptions in the log files.

If you are using an Oracle database, perform all the steps in "Part A - Upgrading the Oracle Database Repository".

If you are using a SQL Server database, skip "Part A - Upgrading the Oracle Database Repository", and perform all the steps in "Part B - Upgrading the SQL Server Database Repository".

B.2.1 Part A - Upgrading the Oracle Database Repository

B.2.1.1 Step 1 Stop the Application Servers

Please make sure to stop all the application servers connected to the Oracle Adaptive Access Manager database.

B.2.1.2 Step 2 Back Up Database Repository

Please make sure to take a full backup of the Oracle Adaptive Access Manager database repository before starting any migration step.

B.2.1.3 Step 3 Run the Setup Scripts

The scripts, which are listed below, are required to upgrade the Oracle Adaptive Access Manager database to the 10.1.4.5 database.

- db_update.sql
- upd_oaam_obj_10145.sql
- oracle_default_locales.sql
- update_locale.sql

db_upgrade.sql

When you run the db_upgrade.sql script, it will automatically run all the other scripts. There is no need to run the scripts manually unless you encounter a problem.

Run this script using the Oracle Adaptive Access Manager repository user.

For example, BRSAADMIN.

The db_upgrade.sql script calls the following scripts

- upd_oaam_obj_10145.sql
- oracle_default_locales.sql
- update_locale.sql

upd_oaam_obj_10145.sql

The upd_oaam_obj_10145.sql script will create or alter objects to support Oracle Adaptive Access Manager 10.1.4.5.

Please check the upd_oaam_obj_10145.log for any error.

Please ignore following errors:

- ORA-01418
- ORA-02260

oracle_default_locales.sql

The oracle_default_locales.sql script will populate the locale table with seed data.

update_locale.sql

The update_locale.sql script will update the V_USER_QUESTION table with locale information.

B.2.1.4 Step 4 Migrate Character Set (Optional)

If you want to convert the database character set from non-unicode characters to unicode, please use the Oracle-provided CSSCAN and CSALTER (Metalink Doc Id: 260192.1).

Basic Steps

The basic steps involved in the character set conversion are listed below.

- BACKUP
- CLUSTER_DATABASE=FALSE (*RAC Only*)
- SHUTDOWN IMMEDIATE
- STARTUP
- CSSCAN
- SHUTDOWN IMMEDIATE
- STARTUP RESTRICT
- CSALTER
- CLUSTER_DATABASE=TRUE (*RAC Only*)
- SHUTDOWN IMMEDIATE
- STARTUP

Conversion Time

The runtime of the character set migration depends on the database size.

Validation

To find the current database character set, run the following SQL statement with DBA credentials. For example, SYS or SYSTEM. (Metalink Doc Note:225938.1)

```
   select value from NLS_DATABASE_PARAMETERS where parameter='NLS_CHARACTERSET'
and value like '%UTF8%'
```

The above query should return at least 1 row if the database character set is set to UTF8.

B.2.2 Part B - Upgrading the SQL Server Database Repository

B.2.2.1 Step 1 Stop Servers

Please make sure to stop all the application servers connected to the Oracle Adaptive Access Manager database.

B.2.2.2 Step 2 Back Up Database Repository

Please make sure to take a full backup of the Oracle Adaptive Access Manager database repository before starting any migration step.

B.2.2.3 Step 3 Run the Setup Scripts

The scripts, which are listed below, are required to upgrade the Oracle Adaptive Access Manager database to the 10.1.4.5 database.

- 001_upgrade_10145_sqlserver.sql
- 055_mssql_default_locales.sql
- 003_update_default_locale.sql

Refer to the following paragraphs for more information on the scripts.

001_upgrade_10145_sqlserver.sql

The 001_upgrade_10145_sqlserver.sql script will create or alter objects to support Oracle Adaptive Access Manager 10.1.4.5.

Run this script on the Oracle Adaptive Access Manager database using the SQL Server Manager console.

Please ignore following warning message:

```
Warning! The maximum key length is 900 bytes.
```

055_mssql_default_locales.sql

The 055_mssql_default_locales.sql script will populate the locale table with seed data.

Run this script on the Oracle Adaptive Access Manager database using the SQL Server Manager console.

003_update_default_locale.sql

The 003_update_default_locale.sql script will update the V_USER_QUESTION table with locale information.

Run this script on the Oracle Adaptive Access Manager database using the SQL Server Manager console.

B.3 Validating the Upgrade Process

To ensure upgrade process is successfully completed, please perform the following steps.

1. Log in to the Oracle Adaptive Access Manager repository.
2. Check the number of tables in the database. There should be 234 tables.
3. Check the entries in vcrypt_db_patches. The database should show entries inserted for 10.1.4.5

```
Select * from vcrypt_db_patches
```

4. Check the application logs for any error.
5. Log in to Adaptive Risk Manager URL (for example: http://test.upgrade.com:9090/oarm) and go to HELP > ONLINE HELP >ABOUT.

   It should say, "Welcome to Oracle Adaptive Access Manager version - 10.1.4.5.xxxxxxx"

B.4 Upgrading Rule Templates and Pre-Existing Models

1. Import the full package of rule conditions (oaam_rule_conditions/oaam_rule_conditions.zip) into Adaptive Risk Manager.
2. Import the saved models into Adaptive Risk Manager.

B.5 Backing Out or Rolling Back the Upgrade Process

In case a failure in the upgrade process occurred or if you have any other reason, you can back out or roll back the upgrade process by following the steps documented below.

1. Stop the Oracle Adaptive Access Manager web applications.
2. Restore the old database backup.
3. Undeploy the newly deployed web applications.
4. Copy and deploy the old backed up web applications.
5. Restart the web applications.
6. Import the rule conditions and saved models.
7. Validate the applications using the Adaptive Risk Manager and Adaptive Strong Authenticator URLs.

C

Upgrading from 3.5 to 10.1.4.3

This appendix contains information about upgrading the Oracle Adaptive Access Manager application and database repository from 3.5 to 10.1.4.3.

If you are upgrading the Oracle Adaptive Access Manager application and database repository from 3.5 to 10.1.4.5, there are two steps involved:

1. Upgrade from 3.5 to 10.1.4.3.
2. Upgrade from 10.1.4.3 to 10.1.4.5

This appendix covers information to upgrade from 3.5 to 10.1.4.3. For information on upgrading from 10.1.4.3 to 10.1.4.5, please refer to Appendix B, "Upgrading from 10.1.4.3 to 10.1.4.5."

C.1 Upgrading the Oracle Adaptive Access Manager Application Layer

In order to upgrade the Oracle Adaptive Access Manager application, please perform the procedures documented in this section.

This section contains the following topics:

- Shut Down and Clean Up Logs
- Back Up the Existing Web Applications
- Deploy and Configure the Web Applications

C.1.1 Shut Down and Clean Up Logs

1. Shut down Oracle Adaptive Access Manager-related web applications.
2. Clean up all old logs.

C.1.2 Back Up the Existing Web Applications

To back up existing web applications:

1. For both Adaptive Strong Authenticator and Adaptive Risk Manager, back up all the properties files under the <WEBAPPS_INSTALLED_DIR>/<WEBAPPS_NAME>/WEB-INF/classes directory to an <UPGRADE_TEMP_DIR> directory. The properties files will be used later in the upgrade process. An example of backing up the files is shown below.

```
Mkdir c:\upgrade_10g_temp
Copy  c:\tomcat\webapp\oarm\WEB-INF\classes c:\upgrade_10g_temp\oarm\classes
```

Note: Ensure that this step is performed because certain property files must be copied back into their respective directories once the new war files have been exploded or unjarred.

2. Back up Oracle Adaptive Access Manager (the deployed application) if you want to upgrade the Oracle Adaptive Access Manager components listed below.
   - Adaptive Strong Authenticator (Authenticator)
   - Adaptive Risk Manager (Tracker)

   You could back up Oracle Adaptive Access Manager applications by renaming the webapps directory or moving the files to a different directory.

Note: This is an important step if you should need to restore an old application or any customer specific customizations.

C.1.3 Deploy and Configure the Web Applications

To deploy and configure the web applications:

1. Copy and explode or unjar the new 10.1.4.3 war files (oasa.war and oarm.war) in the webapps directory. These war files are provided with the upgrade patch.
2. Deploy the web applications.

   Please follow your platform-specific vendor-supplied deployment guide for instructions on how to install web applications.
3. Once your web application is deployed, copy the properties files you saved (during Step 1 of the "Back Up the Existing Web Applications" section) into their respective WEB-INF\classes directories.
   - For the OASA directory (For example, <ASA_HOME>\WEB-INF\classes)
     - bharosa_client.properties
     - bharosa_app.properties
   - For the OARM directory (For example, <ARM_HOME>\WEB-INF\classes)
     - bharosa_server.properties
     - bharosa_app.properties
4. Under the OARM directory (For example, <ARM_HOME>\WEB-INF\classes), modify the bharosa_server.properties by commenting out the following lines.
   - bharosa.hibernate.config.file
   - bharosa.c3p0.config.file
   - bharosa.db.driver
   - bharosa.db.ur
   - bharosa.db.username
   - bharosa.db.password

   Oracle Adaptive Access Manager no longer uses hibernate for object-relational mapping; therefore these lines must be commented out.

5. Since Oracle Adaptive Access Manager 10.1.4.3 uses Oracle's TopLink for object-relational mapping, configure the sessions.xml for the connection manager. First, copy the sample_sessions.xml to sessions.xml under Adaptive Risk Manager's webapps classes directory. For example, <ARM_HOME>\WEB-INF\classes.

   Second, modify sessions.xml by following the directions in Chapter 13, "Configuring Database Connectivity."

C.2 Upgrading the Oracle Adaptive Access Manager Database Repository

The Oracle Adaptive Access Manager database repository must be upgraded as part of the Oracle Adaptive Access Manager upgrade process because the Oracle Adaptive Access Manager database is not backwards-compatible. Ensure that you upgrade the Oracle Adaptive Access Manager repository before starting the newly deployed application; otherwise, exceptions will appear in the log files.

If you are using an Oracle database, perform all the steps in the "Upgrading the Oracle Database Repository" section.

If you are using a SQL Server database, skip the "Upgrading the Oracle Database Repository" section, and perform all the steps in the "Upgrading the SQL Server Database Repository" section.

C.2.1 Upgrading the Oracle Database Repository

Upgrading the Oracle Database Repository involves:

- Backing Up the Oracle Adaptive Access Manager Repository
- Running the Set Up Scripts

Descriptions of the various scripts are also provided in this section for your reference.

C.2.1.1 Backing Up the Oracle Adaptive Access Manager Repository

Please make sure to take a full back up of the Oracle Adaptive Access Manager database repository before starting any migration step.

C.2.1.2 Running the Set Up Scripts

Using SQL*Plus on the database server, run the setup scripts as an Oracle Adaptive Access Manager repository user (For example, BRSAADMIN). The scripts must be run individually and in the following order:

1. upd_oaam_obj_10_1_4_3.sql
2. oracle_default_questions.sql (optional- if required)
3. oracle_answerhints.sql
4. oracle_bharosaconfig.sql
5. oracle_scoringpolicy.sql
6. oracle_validations.sql

After running the scripts, check the upd_oaam_obj_10_1_4.log for any errors.

C.2.1.3 Setup Scripts

The scripts used to upgrade the database for the Adaptive Access Manager database from 3.5 to 10.1.4.3 are described in detail below.

Run these scripts using the Oracle Adaptive Access Manager repository user.

For example, BRSAADMIN.

upd_oaam_obj_10_1_4_3.sql

The upd_oaam_obj_10_1_4_3.sql script will create or alter objects to support Oracle Adaptive Access Manager 10.1.4.3.

oracle_default_questions.sql (Optional)

The oracle_default_questions.sql script will populate the default questions set. Default questions are listed in the script.

Do not run this script if you already have challenge questions enabled.

Modify the script if changes are needed.

oracle_answerhints.sql

The oracle_answerhints.sql script will populate the default answer hints set.

oracle_bharosaconfig.sql

The oracle_bharosaconfig.sql script will populate the Oracle Adaptive Access Manager configuration table with the Oracle Adaptive Access Manager configuration.

oracle_scoringpolicy.sql

The oracle_scoringpolicy.sql script will populate the seed data for challenge question scoring.

oracle_validations.sql

The oracle_validations.sql script will populate the seed data for the validation of the challenge questions.

C.2.2 Upgrading the SQL Server Database Repository

Upgrading the SQL Server database repository involves:

- Backing Up the Oracle Adaptive Access Manager Repository
- Running the Setup Scripts

Descriptions of the various scripts are also provided in this section for your reference.

C.2.2.1 Backing Up the Oracle Adaptive Access Manager Repository

Please make sure you take a full back up of the Oracle Adaptive Access Manager database repository before starting any migration step.

C.2.2.2 Running the Setup Scripts

Please use the SQL Server Management Console to run the setup scripts as an Oracle Adaptive Access Manager repository user (i.e. BRSAADMIN). You must run the scripts individually and in the following order.

1. 001_mssql_upd_oaam_obj_10_1_4_3_sqlserver.sql
2. 060_mssql_default_questions.sql (optional)
3. 070_mssql_scoringpolicy.sql
4. 080_mssql_answerhints.sql

5. 090_mssql_validations.sql
6. 100_mssql_bharosaconfig.sql

C.2.2.3 Setup Script Reference

The SQL scripts used to upgrade the database for the Adaptive Access Manager database from 3.5 to 10.1.4.3 are described below.

001_mssql_upd_oaam_obj_10_1_4_3_sqlserver.sql

This script will create or alter objects to support Oracle Adaptive Access Manager 10.1.4.3.

060_mssql_default_questions.sql (Optional)

This script creates default questions (seed data) as part of the database initialization process. The set of user challenge questions are loaded through this script

> **Note:** Run this script if you are using challenge questions for the first time. If you already have challenge questions enabled, please do not run this script

070_mssql_scoringpolicy.sql

This script will populate the seed data for challenge question scoring.

080_mssql_answerhints.sql

This script will populate the default answer hints set.

090_mssql_validations.sql

This script will populate the seed data for the validation of the challenge questions.

100_mssql_bharosaconfig.sql

This script will populate the Oracle Adaptive Access Manager configuration table with the Oracle Adaptive Access Manager configuration.

C.3 Validating the Upgrade Process

To ensure upgrade process is successfully completed, please perform following steps.

1. Log in to the Oracle Adaptive Access Manager repository.
2. Check the number of tables in the database. There should be 183 tables.
3. Check the entries in vcrypt_db_patches. The database should entries inserted for 10.1.4.3

   ```
   Select * from vcrypt_db_patches
   ```

4. Check the application logs for any error.
5. Log in to Adaptive Risk Manager URL (for example: http://test.upgrade.com:9090/oarm) and go to HELP > ONLINE HELP >ABOUT.

   It should say, "Welcome to Oracle Adaptive Access Manager version - 10.1.4.3.xxxxxxx"

C.4 Backing Out or Rolling Back the Upgrade Process

In case a failure in the upgrade process occurred or for any other reason, you can back out or roll back the upgrade process by following the steps documented below.

1. Stop the Oracle Adaptive Access Manager web applications.
2. Restore the old database backup.
3. Undeploy the newly deployed web applications.
4. Copy and deploy the old backed up web applications.
5. Restart the web applications.
6. Validate the applications using the Adaptive Risk Manager and Adaptive Strong Authenticator URLs.

D

Encryption Reference

A reference for encryption is provided in this appendix.

D.1 Encryption Scheme Definition

Oracle Adaptive Access Manager defines encryption schemes using the "bharosa.cipher.encryption.algorithm.enum" enumeration.

A user defined enumeration is a structured set of properties, that can be treated as a list of objects. Each element in the list may contain several different attributes.

The definition of a user-defined enumeration begins with a property ending in the keyword ".enum" and has a value describing the use of the user-defined enumeration.

Each element definition then starts with the same property name as the enumeration, and adds on an element name. Each enumeration has a value of a unique integer as an ID.

The attributes of the element follow the same pattern, beginning with the property name of the element, followed by the attribute name, with the appropriate value for that attribute.

An example of an enumeration for the "DESede_db" encryption scheme is shown below.

```
bharosa.cipher.encryption.algorithm.enum.DESede_db=22
bharosa.cipher.encryption.algorithm.enum.DESede_db.name=Triple Data Encryption
Standard db
bharosa.cipher.encryption.algorithm.enum.DESede_db.description=Triple Data
Encryption Standard, scheme used of DB sensitive data encryption
bharosa.cipher.encryption.algorithm.enum.DESede_
db.classname=com.bharosa.common.util.cipher.DESedeCipher
bharosa.cipher.encryption.algorithm.enum.DESede_
db.keyRetrieval.classname=com.bharosa.common.util.cipher.KeystoreKeyRetrieval
bharosa.cipher.encryption.algorithm.enum.DESede_
db.passwordRetrieval.classname=com.bharosa.common.util.cipher.SystemKSBase64PassRe
trImpl
bharosa.cipher.encryption.algorithm.enum.DESede_db.alias=DESede_db_key_alias
bharosa.cipher.encryption.algorithm.enum.DESede_db.keystoreFile=system_db.keystore
bharosa.cipher.encryption.algorithm.enum.DESede_db.keystorePassword=
bharosa.cipher.encryption.algorithm.enum.DESede_db.aliasPassword=
```

Attributes of the encryption scheme are shown in the table below:

Attribute	Description	Usage
classname	Implementation of the encryption algorithm.	com.bharosa.common.util.cipher.AESCipher com.bharosa.common.util.cipher.DESedeCipher com.bharosa.common.util.cipher.DESCipher
keyRetrieval	Defines how to retrieve the key for used for encryption.	com.bharosa.common.util.cipher.SystemKeyRetrieval com.bharosa.common.util.cipher.KeystoreKeyRetrieval
keystoreFile	Defines the location of the KeyStore file.	Only applicable if the KeyStore is involved in the retrieval of the key.
passwordRetrieval	Defines how the password to KeyStore and Alias are provided.	com.bharosa.common.util.cipher.SystemKSPassRetrImpl com.bharosa.common.util.cipher.SystemKSBase64PassRetrImpl com.bharosa.common.util.cipher. WebLogicKeyStorePasswordRetrievalImpl
alias	Alias in the KeyStore where the key is stored.	Only applicable if the KeyStore is involved in the retrieval of the key.

The password retrieval options are shown below.

Option	Description
SystemKSPassRetrImpl	Reads the KeyStore and alias passwords from the Oracle Adaptive Access Manager configuration
SystemKSBase64PassRetrImpl	Reads the KeyStore and alias passwords from the Oracle Adaptive Access Manager configuration and expects the passwords to be Base64 encoded
WebLogicKeyStorePasswordRetrievalImpl	Reads the KeyStore and alias passwords from the WebLogic container's provided encryption service

The following schemes are provided pre-configured.

Oracle Adaptive Access Manager Scheme	Algorithm	Keystore Used	Alias	Password Retrieval
DES	DES	system.keystore	DES	SystemKSBase64PassRetrImpl
DESede	DESede	system.keystore	DESede	SystemKSBase64PassRetrImpl
DESede_config	DESede	system_config.keystore	DESede_config_key_alias	SystemKSBase64PassRetrImpl
DESede_db	DESede	system_db.keystore	DESede_db_key_alias	SystemKSBase64PassRetrImpl
AES	AES	system.keystore	AES	SystemKSBase64PassRetrImpl

An example is provided showing the "DESede_db" encryption scheme

```
bharosa.cipher.encryption.algorithm.enum.DESede_db=22
bharosa.cipher.encryption.algorithm.enum.DESede_db.name=Triple Data Encryption
Standard db
bharosa.cipher.encryption.algorithm.enum.DESede_db.description=Triple Data
Encryption Standard, scheme used of DB sensitive data encryption
bharosa.cipher.encryption.algorithm.enum.DESede_
db.classname=com.bharosa.common.util.cipher.DESedeCipher
```

```
bharosa.cipher.encryption.algorithm.enum.DESede_
db.keyRetrieval.classname=com.bharosa.common.util.cipher.KeystoreKeyRetrieval
bharosa.cipher.encryption.algorithm.enum.DESede_
db.passwordRetrieval.classname=com.bharosa.common.util.cipher.SystemKSBase64PassRe
trImpl
bharosa.cipher.encryption.algorithm.enum.DESede_db.alias=DESede_db_key_alias
bharosa.cipher.encryption.algorithm.enum.DESede_db.keystoreFile=system_db.keystore
bharosa.cipher.encryption.algorithm.enum.DESede_db.keystorePassword=
bharosa.cipher.encryption.algorithm.enum.DESede_db.aliasPassword=
```

It is possible to add new schemes using the existing methods. For example, you can use the AES algorithm, read KeyStore and alias passwords from WebLogic container encryption scheme.

Scheme definitions are flexible for adding a new encryption algorithm, algorithm key retrievals, and password retrieval methods by extending Oracle Adaptive Access Manager defined interfaces.

D.2 How the Schemes are Used

The Oracle Adaptive Access Manager configuration checks the property "bharosa.cipher.encryption.algorithm.enum.elem.default" to get the encryption scheme used to encrypt database fields. The default value is "DESede_db". This property is expected to have encryption scheme.

The Oracle Adaptive Access Manager configuration checks the property "bharosa.cipher.encryption.algorithm.enum.elem.system" to get the encryption scheme used to encrypt database fields. The default value is "DESede_config". This property is expected to have encryption scheme.

Integration clients can use "BharosaCipher.getCipher(pEncryptionAlgorithmId)" to work with custom encryption needs. This API expects one of encryption schemes as a parameter.

D.3 Example of Defining a New Encryption Scheme and Using It

```
bharosa.cipher.encryption.algorithm.enum.AES_WL=99
bharosa.cipher.encryption.algorithm.enum.AES_WL.name= AES Scheme using WL password
bharosa.cipher.encryption.algorithm.enum.AES_WL.description= AES Encryption
Standard
bharosa.cipher.encryption.algorithm.enum.AES_
WL.classnameProperty=com.bharosa.common.util.cipher.AESCipher
bharosa.cipher.encryption.algorithm.enum.AES_
WL.keyRetrieval.classname=com.bharosa.common.util.cipher.KeystoreKeyRetrieval
bharosa.cipher.encryption.algorithm.enum.AES_WL.keystoreFile=mykeystore.keystore
bharosa.cipher.encryption.algorithm.enum.AES_
WL.passwordRetrieval.classname=com.bharosa.weblogic.util.cipher.WebLogicKeyStorePa
sswordRetrievalImpl
bharosa.cipher.encryption.algorithm.enum.AES_WL.alias=AES_WL

# Change the scheme used DB sensitive fields encryption with new scheme
bharosa.cipher.encryption.algorithm.enum.elem.default=AES_WL

# (Keystore password=test123, encrypt using WL encryption service)
bharosa.encryption.keystore.password={3DES}vsGNV6Q3YSdfdsfsM=
# (Key password=test123, encrypt using WL encryption service)
bharosa.encryption.keystore.key.password={3DES}vsGNV6Q3YSdfdsfsM=
```

D.4 Creating a Keystore

A KeyStore can store a key used in cryptography in a secure way. Separate passwords to the KeyStore and alias can protect unauthorized access to the key.

Creating and managing a KeyStore is an industry standard. However the "com.bharosa.vcrypt.common.util.KeyStoreUtil" class part of the package provides convenient methods to manage the KeyStore. This utility class takes care of basic KeyStore needs. For advanced needs, refer to the Java Spec.

Usage: java <OARM_INSTAL_DIR>/WEB-INF/lib/ com.bharosa.vcrypt.common.util.KeyStoreUtil <command> readFromFile=<file name>

Useful Commands

Command	Description
WriteKeyToFile	Write secret key from KeyStore to a file
UpdateOrCreateKeyStore	Creates or updates a KeyStore with the key provided
UpdateOrCreateKeyStoreWithAutoGeneratedKey	This command first generates a key based on the algorithm specified. The generated key is stored in the KeyStore
base64encode	Encodes passwords using Base64
base64decode	Decodes passwords using Base64

Parameters

Parameter	Description
keystorefilename	Name of the KeyStore file to be created / updated.
keystoretype	Type of KeyStore JCEKS, JKS
keystorepasswd	Password of the KeyStore
keystorealias	Alias Name
keystorealiaspasswd	Password to access the alias
keyfile	File in which the secret key is stored
algorithm	Algorithm DES, DESede, DES
tobase64	Value to encode to base64
frombase64	Value to decode using base64, expects encoded value as parameter
Printencodedpasswords	Prints encoded KeyStore and alias passwords along with KeyStore creation / updates.
writetofilename	File name where key has to be written

D.5 Secret Key

Key used for encryption / decryption of passwords. Different algorithms have different key needs. Make sure to provide proper key based on algorithm used. To use AES with 192 or 256 key sizes, refer to JVM provider.

E

Archive and Purge

This appendix contains information about the archive and purge process.

E.1 Overview

This section presents the concepts, prerequisites, policy, and post-process procedures in archiving and purging the Oracle Adaptive Access Manager database. A DBA or system administrator, who performs routine maintenance and the archiving and purging of the Oracle Adaptive Access Manager database, should follow the instructions in this chapter.

The overview section contains the following topics:

- Purge Process
- Archive Process
- Archive and Purge Data Classification

E.1.1 Purge Process

Purging is the process of freeing up space in the database or of deleting obsolete data that is not required by the system. The purge process can be based on the age of the data or the type of data.

E.1.2 Archive Process

Archiving is the process of backing up the obsolete data that will be deleted during the purge process. During the archive process, data will be moved from the main transactional tables to the backup tables. By default the Oracle Adaptive Access Manager purge scripts will archive data that will be deleted during the purge process.

E.1.3 Archive and Purge Data Classification

Oracle Adaptive Access Manager has different sets of transactional tables that will be archived and purged. These sets are documented below. The tables in the transaction table sets are listed in "List of Tables and the Corresponding Archived Tables".

E.1.3.1 Device Fingerprinting

The device fingerprinting data is archived and purged based on the following criteria:

- archive and purge the device fingerprinting logs that are older than a specified period first.

- archive and purge user device maps that are not used after the data from the device fingerprinting logs is purged.
- archive and purge the device history that is not used after the data from the device fingerprinting logs is purged.
- archive and purge the device data that is not used after the data from the device fingerprinting logs is purged.

E.1.3.2 Transaction In-Session Based Data

The in-session transaction data is archived and purged based on the following criteria:

- archive and purge the in-session transactional-based data that is older than a specified period first.
- archive and purge transaction data that is not used in the transaction data after the transactions logs are purged for a specific time period.
- archive and purge the entity, entity profile, user entity map and entity transaction map after the transactions logs are purged for a specific time period.

E.1.3.3 Auto-learning Profile Data

The Auto-learning and profile data is archived and purged based on the following criteria:

- archive and purge the Workflow tables based on a specific time period.
  - HOURS based Workflow tables will retain 3 days' worth of data.
  - DAYS based Workflow tables will retain 32 days' worth of data.
  - MONTHS based Workflow tables will retain 1 year's worth of data.
  - YEARS based Workflow tables will retain 5-years' worth of data.

  These values are hardcoded. The profile data value can be changed in the execution script for no of days.
- archive and purge fingerprinting data with fingerprint type 11, 12, and no child records in the Workflow tables

  ```
  vcrypt.fingerprint.type.enum.autolearning.auth=11
  vcrypt.fingerprint.type.enum.autolearning.transaction=12
  ```

  - 11 is the enum value for the Auto-learning AUTH type. Change these values in the script if another value was used during integration.
  - 12 is enum value for the Auto-learning TRANSACTION type. Change these values in the script if another value was used during integration.
- archive and purge profile related data that is 183 days old and profiles type 2 (Auto-learning Profile) from the Auto-learning profiles tables.

E.1.3.4 Rule Log Data

The rule log transaction data is archived and purged based on the following criteria:

- archive and purge the rule log data that is 30 days old

E.2 Archive and Purge

E.2.1 Setting Up for Archive and Purge

The setup scripts are one-time scripts that are required to create objects for the archive and purge process. The setup scripts will create the archived tables and store procedure required to execute during the routine archive and purge process.

E.2.1.1 Setting Up for Archive and Purge for the Oracle Database

The required scripts to setup the archive and purge routines for the Oracle database are listed below. For more information on these scripts, refer to "Scripts for the Oracle Database"

To set up the archive and purge process for the Oracle database, follow the steps below:

1. Create the script directory, oaam_purge_script.
2. Unzip the Oracle Adaptive Access Manager purge package Oracle scripts to the script directory.
3. Login to the database using the Oracle Adaptive Access Manager schema

   ```
   For example, sqlplus <OAAMADMIN>/<PASSWORD>
   ```

4. Run the create_purge_proc.sql script

   ```
   SQL>@ create_purge_proc.sql
   ```

E.2.1.2 Setting Up for Archive and Purge for the SQL Server Database

The required scripts to setup the archive and purge routines for the SQL Server database are listed below. For more information on these scripts, refer to "Scripts for the SQL Server Database".

- cr_vcrypt_purge_tables.sql
- cr_sp_arch_purge_tracker_data.sql
- cr_sp_arch_purge_txn_logs.sql
- cr_sp_arch_purge_workflow_data.sql
- cr_sp_arch_purge_profile_data.sql
- cr_sp_arch_purge_rules_log.sql

To setup the archive and purge process for the SQL Server database, follow the steps below:

1. Create the script directory, oaam_purge_script.
2. Unzip the Oracle Adaptive Access Manager purge package SQL Server scripts to the script directory.
3. Login to the Oracle Adaptive Access Manager database using SQL Server Management Studio.
4. Open the script files, which are listed below, using File ->Open ->File. Then, navigate to the script directory.
   - cr_vcrypt_purge_tables.sql
   - cr_sp_arch_purge_tracker_data.sql
   - cr_sp_arch_purge_txn_logs.sql
   - cr_sp_arch_purge_workflow_data.sql

- cr_sp_arch_purge_profile_data.sql
- cr_sp_arch_purge_rules_log.sql

5. In the Query window, change the following line for every script:

```
USE [DATABASE_NAME] to USE < your OAAM Database>
```

6. Execute the scripts.
7. In the message window of SQL Server Management Studio, save the results to a file.

E.2.2 Performing Archive and Purge

The execution of the archive and purge scripts is described below. Prior to starting the archive and purge process, go through the checklist, which is documented below, to ensure that the requirements for archive and purge are met.

- Setup of the archive and purge scripts. Refer to "Setting Up for Archive and Purge".
- Enough space is available on the database server to store the archived data, if archive is enabled for the purge.
- Archive and purge could be resource (like CPU) intensive. Oracle recommends running these during off peak load hours.

E.2.2.1 Oracle Databases

The required scripts to execute archive and purge routines for the Oracle database are listed below. For more information on these scripts, refer to "Scripts to Execute Archive and Purge".

Archive and purge periods are set based on the business requirement specified for retention periods.

By default, the archive and purge scripts/routines have the following two parameters set:

- p_days1 =no of days for data retention
- p_archived= archived flag

To change these values per the business requirement, modify the following scripts:

- exec_sp_purge_tracker_data.sql
- exec_sp_purge_txn_log.sql
- exec_sp_purge_workflow_data.sql
- exec_sp_purge_profile_data.sql
- exec_sp_purge_rule_log.sql

E.2.2.1.1 Manual Execution To execute the scripts to archive and purge, follow the steps below:

1. Create the script directory, oaam_purge_script
2. Unzip the Oracle Adaptive Access Manager archive and purge package Oracle scripts to the script directory.
3. Login to the database using the Oracle Adaptive Access Manager schema

For example,

```
sqlplus <OAAMADMIN>/<PASSWORD>
```

4. Run the purging execution scripts:

```
SQL>@ exec_sp_purge_tracker_data.sql
SQL>@ exec_sp_purge_txn_log.sql
SQL>@ exec_sp_purge_workflow_data.sql
SQL>@ exec_sp_purge_profile_data.sql
SQL>@ exec_sp_purge_rule_log.sql
```

E.2.2.1.2 Automatic Scheduling Archive and purge jobs should be part of a routine schedule. These jobs can be scheduled using database jobs or OS-based scheduling utilities (crontab, at) or scheduler software (autosys, appworx).

It is recommended that these scripts are scheduled to run on regular intervals and only during off-peak hours.

E.2.2.2 SQL Server Database

The required scripts to execute archive and purge routines are listed below. For more information about these scripts, refer to "Scripts to Execute Archive and Purge".

Archive and purge periods are set based on the business requirement specified for retention periods.

By default, the required scripts for archive and purge routines have the following two parameters set:

- p_days1 =no of days for data retention
- p_archived= Archived flag

To change these values per the business requirement, modify the following scripts:

- exec_sp_purge_tracker_data.sql
- exec_sp_purge_txn_log.sql
- exec_sp_purge_workflow_data.sql
- exec_sp_purge_profile_data.sql
- exec_sp_purge_rule_log.sql

E.2.2.2.1 Manual Execution To execute the scripts to archive and purge, follow the steps below:

1. Create the script directory, oaam_purge_script.
2. Unzip the Oracle Adaptive Access Manager archive and purge package SQL Server scripts to the script directory.
3. Login to the Oracle Adaptive Access Manager database using SQL Server Management Studio.
4. Open the script files listed below using File ->Open ->File. Then, navigate to the script directory.

```
exec_sp_purge_tracker_data.sql
exec_sp_purge_txn_log.sql
exec_sp_purge_workflow_data.sql
exec_sp_purge_profile_data.sql
exec_sp_purge_rule_log.sql
```

5. In the Query window, change the following line for every script:

```
USE [DATABASE_NAME] to USE < your OAAM Database>
```

6. Execute the scripts.
7. In the message window of the SQL Server Management Studio, save the results to a file.

E.2.2.2.2 Automatic Scheduling Archive and purge jobs should be part of a routine schedule. These jobs can be scheduled using database jobs or OS-based scheduling utilities (crontab, at) or scheduler software (autosys, appworx).

It is recommended that these scripts are scheduled to run on regular intervals and only during off-peak hours.

E.3 Validating Archive and Purge

To determine if the archive and purge was successful, check the log files (for example scheduler log, script output log, and others) for any errors. When the archive and purge process has completed, users can also query the transactional log and its related purged tables to validate that the data was archived and purged.

E.4 Restoring Archived Data

As recommended, users should take an export backup of archived tables after the archive process has completed in case they should need to perform troubleshooting in the future.

When performing a restoration, the user should restore the desired date's data to a temporary table using Oracle's database Import feature.

Please contact Oracle Support if any data restoration is required.

E.5 List of Tables and the Corresponding Archived Tables

E.5.1 Device Fingerprint Tables and Corresponding Archived Tables

Device Fingerprint Transaction Tables	Corresponding Archived Tables
VCRYPT_TRACKER_NODE	VCRYPT_TRACKER_NODE_PURGE
VCRYPT_TRACKER_NODE_HISTORY	VCRYPT_TRACKER_NODE_HISTORY_PURGE
VCRYPT_TRACKER_USERNODE_LOGS	VCRYPT_TRACKER_USERNODE_LOGS_PURGE
VT_DYN_ACT_EXEC_LOG	VT_DYN_ACT_EXEC_LOG_PURGE
VT_SESSION_ACTION_MAP	VT_SESSION_ACTION_MAP_PURGE
VT_USER_DEVICE_MAP	VT_USER_DEVICE_MAP_PURGE

E.5.2 Auto-learning Transactional Tables and Corresponding Archive Tables

Auto-learning Transactional Tables	Corresponding Archived Tables
VT_WF_DAYS	VT_WF_DAYS_PURGE
VT_WF_HOURS	VT_WF_HOURS_PURGE
VT_WF_MONTHS	VT_WF_MONTHS_PURGE
VT_WF_YEARS	VT_WF_YEARS_PURGE
V_FPRINTS	V_FPRINTS_PURGE
V_FP_MAP	V_FP_MAP_PURGE
VT_USER_PROFILE	VT_USER_PROFILE_PURGE
VT_DEVICE_PROFILE	VT_DEVICE_PROFILE_PURGE
VT_IP_PROFILE	VT_IP_PROFILE_PURGE
VT_STATE_PROFILE	VT_STATE_PROFILE_PURGE
VT_CITY_PROFILE	VT_CITY_PROFILE_PURGE
VT_COUNTRY_PROFILE	VT_COUNTRY_PROFILE_PURGE

E.5.3 Transaction Tables and Corresponding Archived Tables

Transaction Tables	Corresponding Archived Tables
VT_ENTITY_ONE	VT_ENTITY_ONE_PURGE
VT_ENTITY_ONE_PROFILE	VT_ENTITY_ONE_PROFILE_PURGE
VT_ENT_TRX_MAP	VT_ENT_TRX_MAP_PURGE
VT_TRX_DATA	VT_TRX_DATA_PURGE
VT_TRX_LOGS	VT_TRX_LOGS_PURGE

E.5.4 Rule Logs Tables and Corresponding Archived Tables

Rule Log Tables	Corresponding Archived Tables
VR_POLICYSET_LOGS	VR_POLICYSET_LOGS_PURGE
VR_RULE_LOGS	VR_RULE_LOGS_PURGE
VR_MODEL_LOGS	VR_MODEL_LOGS_PURGE
VR_POLICY_LOGS	VR_POLICY_LOGS_PURGE

E.6 Scripts to Set Up Archive and Purge

E.6.1 Scripts for the Oracle Database

E.6.1.1 create_purge_proc.sql

The create_purge_proc.sql script creates the tables (Listed in "List of Tables and the Corresponding Archived Tables") and the following stored procedures to archive and purge data from the transaction tables:

- SP_RULE_ PROC
- SP_MODEL_ PROC
- SP_POLICYSET_ PROC
- SP_POLICY_ PROC
- SP_NODE_HISTORY_ PROC
- SP_NODE_PROC
- SP_USER_NODE_PROC
- SP_USER_DVC_PROC
- SP_SESS_ACT_MAP_PROC
- SP_WF_YEARS_PROC
- SP_WF_MONTHS_PROC
- SP_WF_DAYS_PROC
- SP_WF_HOURS_PROC
- SP_V_FPRINTS_PROC
- SP_V_FP_MAP_PROC
- SP_VT_TRX_LOGS_PROC
- SP_VT_TRX_DATA_PROC
- SP_VT_ENT_TRX_MAP_PROC
- SP_VT_ENT_ONE_PRF_PROC
- SP_VT_ENT_ONE_PROC
- SP_VT_ENT_ONE_MAP_PROC
- SP_VT_USER_PRF_PROC
- SP_VT_DEVICE_PRF_PROC
- SP_VT_IP_PRF_PROC
- SP_VT_BASE_IP_PRF_PROC
- SP_VT_CITY_PRF_PROC
- SP_VT_COUNTRY_PRF_PROC
- SP_VT_STATE_PRF_PROC

E.6.2 Scripts for the SQL Server Database

E.6.2.1 cr_vcrypt_purge_tables.sql

The cr_vcrypt_purge_tables.sql script creates the tables ("List of Tables and the Corresponding Archived Tables") to archive and purge data from the transaction tables.

E.6.2.2 cr_sp_arch_purge_tracker_data.sql

The cr_vcrypt_purge_tables.sql script creates the stored procedure sp_archive_purge_tracker_data to archive and purge data from device fingerprinting transaction tables.

E.6.2.3 cr_sp_arch_purge_txn_logs.sql

The cr_vcrypt_purge_tables.sql script creates the stored procedure sp_archive_purge_txn_logs_data to archive and purge data from in-session transaction tables.

E.6.2.4 cr_sp_arch_purge_workflow_data.sql

The cr_vcrypt_purge_tables.sql script creates the stored procedure sp_archive_purge_wf_data to archive and purge data from work flow transaction tables.

E.6.2.5 cr_sp_arch_purge_profile_data.sql

The cr_vcrypt_purge_tables.sql script stored procedure sp_archive_purge_profile_data to archive and purge data from Auto-learning profile transaction tables.

E.6.2.6 cr_sp_arch_purge_rules_log.sql

The cr_vcrypt_purge_tables.sql script creates the stored procedure sp_archive_purge_rule_log to archive and purge data from rule logs transaction tables.

E.7 Scripts to Execute Archive and Purge

E.7.1 exec_sp_purge_tracker_data.sql

This script calls stored procedures to archive and purge data from device fingerprinting tables. By running this script, the following tables will be archived and purged:

- VCRYPT_TRACKER_NODE
- VCRYPT_TRACKER_NODE_HISTORY
- VCRYPT_TRACKER_USERNODE_LOGS
- VT_USER_DEVICE_MAP
- VT_DYN_ACT_EXEC_LOG
- VT_SESSION_ACTION_MAP

E.7.2 exec_sp_purge_txn_log.sql

This script calls stored procedures to archive and purge data from in-session transaction tables. By running this script, the following tables will be archived and purged:

- VT_ENTITY_ONE
- VT_ENTITY_ONE_PROFILE
- VT_ENT_TRX_MAP
- VT_TRX_DATA
- VT_TRX_LOGS
- VT_USER_ENTITY1_MAP

E.7.3 exec_sp_purge_workflow_data.sql

This script calls stored procedures to archive and purge data from the Workflow Auto-learning tables. By running this script, the following tables will be archived and purged:

- VT_WF_DAYS
- VT_WF_HOURS
- VT_WF_MONTHS
- VT_WF_YEARS
- V_FPRINTS
- V_FP_MAP

E.7.4 exec_sp_purge_profile_data.sql

This script calls stored procedures to archive and purge data from the Auto-learning profile tables. By running this script, the following tables will be archived and purged:

- VT_BASE_IP_PROFILE
- VT _IP_PROFILE
- VT_DEVICE_PROFILE
- VT_COUNTRY_PROFILE
- VT_CITY_PROFILE
- VT_STATE_PROFILE
- VT_USER_PROFILE

E.7.5 exec_sp_purge_rule_log.sql

This script calls stored procedures to archive and purge data from the Rules Engine logging tables. By running this script, the following tables will be archived and purged:

- VR_POLICYSET_LOGS
- VR_RULE_LOGS
- VR_MODEL_LOGS
- VR_POLICY_LOGS

E.8 Purging Guidelines

E.8.1 When to Perform Archive and Purge

In order to maintain data consistency and optimal system performance, users should perform the purging/archiving process routinely.

E.8.2 Minimum Data Retention Policy

Based on the Oracle Adaptive Access Manager system requirement, the minimum data retention policy for various OLTP tables are shown below, but users should determine

the data retention period based on their business requirements. For more information, review the information in this chapter.

E.8.2.1 Device Fingerprinting Data

Minimum of 6 months or 180 days

E.8.2.2 In-session Transactional Tables

Minimum of 6 months or 180 days

E.8.2.3 Auto-learning and Workflow Tables

- HOURS based Workflow tables will retain 3 days' worth of data.
- DAYS based Workflow tables will retain 32 days' worth of data.
- MONTHS based Workflow tables will retain 1 year's worth of data.
- YEARS based Workflow tables will retain 5-years' worth of data.

E.8.2.4 Rule Log Data

The script will archive and purge all rule log data that is 30 days older (This value should be set based on the customer care requirement. If the reporting database is used, then, rule logging data retention should be less than 30 days.

E.8.3 Special Requirements

- Set up of the archive and purge scripts.
- Ensure that enough space is available on the database server to store the archived data, if archival is enabled during purging.
- Archival and purging could be resource (like CPU) intensive. Oracle recommends running these during off peak load hours.

E.8.4 Purging Validation

To determine if the archive and purge had been successful, check the log files (for example scheduler log, script output log, and others) for any errors. Transactional log tables can also be queried to validate the data for the purging process.

F

Rule Logging

Rule logging records the required rule processing information so that the Rule Administrator can monitor the required information from a user session.

F.1 Configuration Controls

The properties used to enable/disable and specify the Runtime for Rule logging are listed below.

```
vcrypt.tracker.rules.trace.policySet=[true|false]
vcrypt.tracker.rules.trace.policySet.<runtime string value>=[true|false]
```

Use the Properties Editor to edit these properties.

F.2 Scenario

In the scenario, the Post-Authentication Runtime will be used. The Runtime string value for

```
profile.type.enum.postauth.name=Post-Authentication
```

is "postauth".

F.2.1 How It Works

The flow of how Rule logging works is as follows:

1. The Rules Engine first checks to see if a configuration exists for `vcrypt.tracker.rules.trace.policySet.postauth`.
2. If there is no configuration value set, the Rules Engine will check the configuration value of `vcrypt.tracker.rules.trace.policySet`.

The default value for `vcrypt.tracker.rules.trace.policySet` is "true".

F.2.2 Cases

The matrix below shows an example of how value combinations control logging during a specified Runtime.

value of vcrypt.tracker.rules.trace.policySet.postauth	value of vcrypt.tracker.rules.trace.policySet	Will Rule logging be enabled for the postauth Runtime?
true	false	yes

value of vcrypt.tracker.rules.trace.policySet.postauth	value of vcrypt.tracker.rules.trace.policySet	Will Rule logging be enabled for the postauth Runtime?
true	true	yes
true	not set	yes
false	false	no
false	true	no
false	not set	no
not set	false	no
not set	true	yes
not set	not set	yes

F.2.3 Main Point of Scenario

The main point of the scenario is that if the logging configuration is explicitly set at the given Runtime, the Rules Engine uses that value; otherwise, it uses the parent's value.

F.3 How to Control What Rules Are Logged:

The properties to control which Rules are logged are shown below.

```
vcrypt.tracker.rules.trace.notTriggered=[true|false]
vcrypt.tracker.rules.trace.notTriggered.logMillis=[millis]
```

If `vcrypt.tracker.rules.trace.notTriggered` is set to "true," Rules that are not triggered are also logged.

The value of `vcrypt.tracker.rules.trace.notTriggered.logMillis` will narrow down which Rules are shown.

If the Rule execution for non-triggered Rules exceeds the value of `vcrypt.tracker.rules.trace.notTriggered.logMillis`, only then will the Rules Engine log the non-triggered Rules.

F.4 Examples

The table below shows the property values that control what Rules get logged.

vcrypt.tracker.rules.trace.notTriggered	vcrypt.tracker.rules.trace.notTriggered.logMillis	Result
true	n	Logs the non-triggered Rules that took more than "n". If "n" is set to a negative value, all Rules are logged
false	n	None of the non-triggered Rules will be logged

G

10.1.4.3 vs. 10.1.4.5 Features

This appendix contains a feature comparison matrix for 10.1.4.3 and 10.1.4.5.

Features	10.1.4.3	10.1.4.5
Real-time and offline rules engine	X	X
Virtual authentication devices	X	X
Knowledge-based authentication	X	X
Adaptive device identification*	X	X
Base security models (ongoing updates)	X	X
Real-time dashboard (improved)	X	X
Customer service module	X	X
Real-time reporting	X	X
Standard actions, alerts, and risk scoring	X	X
Standard rule templates	X	X
Standard rule conditions		X
Behavior bucketing (reduces data volumes)		X
Optimized log data management		X
Enhanced caching of rules data object		X
Expanded integration APIs		X
Investigation agent workflow		X
Rules authoring user interface		X
Transaction definition and mapping user interface		X
Data entity definition and mapping user interface		X
Behavior pattern capture user interface		X
Configurable Actions		X
OTP via SMS and email out-of-band authentication		X
Customizable reporting BI Publisher (bundled)		X
Globalization		X
WebLogic (bundled with Oracle Adaptive Access Manager)		X

Integrations	10.1.4.3	10.1.4.5
Oracle Access Manager integration	X	X
Oracle Entitlements Server integration		X
Oracle Flexcube core banking		X
Oracle Applications integrations		X
Juniper SSL VPN integration		X

Index

J

L

M

N

O

P

R

S

T

U

W