Oracle® Fusion Middleware

Integration Guide for Oracle Access Manager

11g Release 1 (11.1.1)

E15740-05

July 2013

ORACLE

Oracle Fusion Middleware Integration Guide for Oracle Access Manager, 11g Release 1 (11.1.1)

E15740-05

Primary Author: Gail Flanegin

Contributing Author: Priscilla Lee, Vinaye Misra

Contributors: Aarathi Balakrishnan, Sagar Bongale, Bob Bradee, Damien Carru, Vikas Pooven Chathoth, Sree Chitturi, Toby Close, Ellen Desmond, Gail Flanegin, Don Gosselin, Mark Karlstrand, Ari Kermaier, Ashish Kolli, Svetlana Kolomeyskaya, Vadim Lander, Wei Jie Lee, Derick Leo, Madhu Martin, Sergio Mendiola, Vamsi Motukuru, Srinivas Nagandla, Maya Neelakandhan, Madhan Neethiraj, Jeff Nester, Rey Ong, Deepak Ramakrishnan, Rajiv Sharma, Kamal Singh, Shyam Singh, Saai Soundararajanshanthibai, Elangovan Subramanian, Dawn Tyler, Catherine Wong

Contents

7 Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager

List of Figures

List of Tables

Preface

The *Oracle Fusion Middleware Integration Guide for Oracle Access Manager* describes how to integrate other Oracle Identity Management products with Oracle Access Manager.

Audience

This document is intended for administrators who are familiar with the following:

- Oracle WebLogic Server concepts and administration
- Concepts and administration of these Oracle Identity Management components:
  - Oracle Identity Manager
  - Oracle Adaptive Access Manager
  - Oracle Identity Navigator
  - Oracle Identity Federation
- LDAP directory configuration and administration
- Web server concepts and administration
- WebGate and mod_osso agents

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

- *Oracle Access Manager 11g Release 1 (11.1.1) Release Notes*

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*—Explains install-time integration of Oracle Identity Management components
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service* —Describes daily administration and policy configuration tasks using Oracle Access Manager
- *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Upgrade Planning Guide*
- *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Administrator's Guide*—Describes how to manage Oracle Fusion Middleware, including how to change ports, how to deploy applications, and how to back up and recover Oracle Fusion Middleware. This guide also explains how to move data from a test to a production environment.
- *Oracle Fusion Middleware Application Security Guide*—Explains deploying Oracle Access Manager 10g SSO solutions, which have been replaced by OAM 11g SSO.
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*—provides reference deployment scenarios.
- *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*—Provides a section on customized Oracle Access Manager commands in the chapter "Infrastructure Security Custom WLST Commands".

Conventions

The following text conventions are used in this document:

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

What's New in Oracle Access Manager?

This chapter lists new integration features and updates.

What's New in 11g Release 1 (11.1.1.7.0)

Updates information for Service Provider Integration Modules in Chapter 4, "Integrating Oracle Identity Federation".

What's New in 11g Release 1 (11.1.1.5.0)

New Integration Features

A new integration tool is available in this release to help automate certain integration steps.

New Topics in this Guide

This guide contains the following new and updated topics:

- Chapter 5 explains how to integrate Oracle Access Manager and Oracle Identity Manager using the integration automation tool.
- The procedures for integrating with Oracle Identity Manager and Oracle Adaptive Access Manager in Chapter 6 and Chapter 7 have been revised.
- Chapter 8 shows how to integrate 10*g* Oracle Access Manager with 11*g* Oracle Adaptive Access Manager.

What's New in 11g Release 1 (11.1.1)

New Features in Oracle Access Manager

For a description of new features in Oracle Access Manager, see Introduction to Oracle Access Manager 11g and Administration in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

New Integrations

This release supports integrations with the following Oracle Identity Management components:

- Oracle Identity Manager
- Oracle Adaptive Access Manager

- Oracle Identity Federation
- Oracle Identity Navigator

Additional Topics

This edition of the document provides a section to help you understand identity management perspectives. See Section 2.1.

1

About Oracle Identity Management Components

This chapter provides an overview of the components with which Oracle Access Manager 11g Release 1 (11.1.1) integrates. For an introduction to Oracle Access Manager, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

This chapter contains these sections:

1.1 About Oracle Access Manager Integrations

Integrating Oracle Access Manager 11g Release 1 (11.1.1) with other applications and portals requires some knowledge of both products. This guide provides the information required to set up Oracle Access Manager for specific applications and components you can integrate with Oracle Access Manager.

1.2 A Note About IDMDomain Agents and Webgates

By default, the IDMDomain Agent is enabled in the Oracle HTTP Server deployment. If you migrate from IDMDomain Agent to WebGate Agent, note the following:

- The protection policies set up for IDMDomain can be reused for WebGate if your webgate uses the IDMDomain preferredHost.
- IDMDomain and WebGate can coexist. If the IDMDomain Agent discovers a WebGate Agent in the Oracle HTTP Server deployment, IDMDomain Agent becomes dormant.

> **See Also:** Configuring Centralized Logout for the IDM Domain Agent in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

1.3 Components Described in This Document

This section provides a brief survey of the Oracle Identity Management components that integrate with Oracle Access Manager. They are:

- Oracle Identity Navigator
- Oracle Identity Federation
- Oracle Identity Manager
- Oracle Adaptive Access Manager

1.3.1 Oracle Identity Navigator

Oracle Identity Navigator is a web-based application that you access through a browser. You can use it to access consoles for Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Manager, Directory Services (ODSM), and other Oracle Identity Management services.

For details about integration with Oracle Access Manager, see Chapter 3, "Integrating with Oracle Identity Navigator".

1.3.2 Oracle Identity Federation

Oracle Identity Federation is a complete, enterprise-level and carrier-grade solution for secure identity information exchange between partners. Oracle Identity Federation protects existing IT investments by integrating with a wide variety of data stores, user directories, authentication providers and applications.

For details about integration with Oracle Access Manager, see Chapter 4, "Integrating Oracle Identity Federation".

1.3.3 Oracle Identity Manager

Oracle Identity Manager is a powerful and flexible enterprise identity management system that automatically manages users' access privileges within enterprise IT resources. Oracle Identity Manager is designed from the ground up to manage user access privileges across all of a firm's resources, throughout the entire identity management lifecycle—from initial creation of access privileges to dynamically adapting to changes in business requirements.

For details about integration with Oracle Access Manager, see Chapter 7, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager".

1.3.4 Oracle Adaptive Access Manager

Oracle Adaptive Access Manager is Oracle Identity Management's solution for web access real-time fraud detection and multifactor online authentication security for the enterprise.

For details about integration with Oracle Access Manager, see:

- Chapter 6, "Integrating Oracle Access Manager and Oracle Adaptive Access Manager".
- Chapter 7, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager".
- Chapter 8, "Integrating Oracle Access Manager 10g and Oracle Adaptive Access Manager 11g"

1.4 System Requirements and Certification

Refer to the system requirements and certification documentation for information about hardware and software requirements, platforms, databases, and other information. Both of these documents are available on Oracle Technology Network (OTN).

The system requirements document covers information such as hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-requirements-100147.html

The certification document covers supported installation types, platforms, operating systems, databases, JDKs, directory servers, and third-party products:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

2

Introduction to Oracle Access Manager Integrations

This chapter introduces the integrations between Oracle Access Manager and other components of the Oracle Identity Management suite, including interaction flows among the components, high level requirements for each integration, and related information.

This chapter contains these sections:

Note: Integration procedures are described elsewhere in this document. See Section 2.2, "Summary of Integrations".

See Also: Section 1.2, "A Note About IDMDomain Agents and Webgates".

2.1 Perspectives on Identity Management Integration

At the outset it is useful to consider different approaches to integrating the various Oracle Identity Management components.

2.1.1 Access Management Perspective

A common starting point is to adopt an Oracle Access Manager perspective with intranet/extranet SSO. From this perspective, you may want to simply enable user

management/registration into the LDAP directory with which Oracle Access Manager works.

In this scenario you do not need enterprise provisioning but rather focus on management of users in the LDAP directory. The requirements include tasks like integrating the login page (forgotten password link), setup/detection of password policies, password-must-change redirects, tracking password history, deploying schema for password/account attributes, and so on.

This integration is primarily centered around access management with Oracle Access Manager. In this deployment Oracle Access Manager and Oracle Identity Manager could be in the same Oracle WebLogic Server domain, but you may wish to set up two different domains. User registration workflows usually have workflow enabled.

2.1.2 Oracle Identity Manager Perspective

From the Oracle Identity Manager (provisioning) perspective, we wish to use Oracle Access Manager as the SSO solution for Oracle Identity Manager as well as other applications.

In this configuration Oracle Identity Manager is protected by an agent or asserter and participates in the corporate SSO domain.

2.1.3 Additional Perspectives

Beyond identity and access, additional perspectives apply to sites needing federated single sign-on and advanced access management.

Here, the SSO infrastructure needs to be federated (by means of Oracle Identity Federation, bringing in Oracle Access Manager/Oracle Identity Federation integration); or strengthened (by means of Oracle Adaptive Access Manager, bringing in and Oracle Access Manager/Oracle Adaptive Access Manager integration).

2.2 Summary of Integrations

Table 2–1 lists the identity management integrations described in this document.

Table 2–1 Summary of Oracle Access Manager Integrations

Integration	Components	Additional Information
Identity Administration and Access Control	Oracle Identity Manager Oracle Access Manager	Section 2.3, "Enabling Identity Administration with Oracle Identity Manager"
Protecting the Oracle Identity Manager Console	Oracle Identity Manager Oracle Access Manager	Section 2.4, "Enabling Single Sign-On for Oracle Identity Manager"
Protecting the Oracle Identity Navigator Console	Oracle Identity Navigator Oracle Access Manager	Chapter 3, "Integrating with Oracle Identity Navigator"

Table 2–1 (Cont.) Summary of Oracle Access Manager Integrations

Integration	Components	Additional Information
Pre- and Post-Authentication	Oracle Adaptive Access Manager	Chapter 6, "Integrating Oracle Access Manager and Oracle Adaptive Access Manager"
	Oracle Access Manager	
Authentication in Federation Environment	Oracle Access Manager Oracle Identity Federation	Chapter 4, "Integrating Oracle Identity Federation"
Advanced Authentication and Password Management	Oracle Adaptive Access Manager	Chapter 7, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager"
	Oracle Access Manager	
	Oracle Identity Manager	

2.3 Enabling Identity Administration with Oracle Identity Manager

Oracle Identity Manager provides identity administration services for Oracle Fusion Middleware.

Integration enables you to manage identities with Oracle Identity Manager and control access to resources with Oracle Access Manager. As explained later in this chapter, you can then implement single sign-on for other identity management components and perform additional integrations with suite components.

The prerequisites for integrating with Oracle Identity Manager are:

- installing the necessary components/suites, which include: Repository Creation Utility (RCU), Oracle WebLogic Server, the IAM Suite, and Oracle SOA Suite
- creating schemas for Oracle Identity Manager and Oracle SOA Suite
- installing and configuring Oracle Internet Directory and Oracle Virtual Directory
- uploading the password schemas to Oracle Internet Directory

After meeting the prerequisites, the basic integration steps are as follows:

1. Create the Oracle WebLogic Server domains for Oracle Access Manager and Oracle Identity Manager/Oracle SOA Suite respectively.
2. Install Oracle HTTP Server 11*g*.
3. Configure Oracle Access Manager 11*g* to point to Oracle Internet Directory rather than to the default embedded LDAP.

For integration details, see Chapter 5, "Integrating Oracle Access Manager and Oracle Identity Manager".

2.4 Enabling Single Sign-On for Oracle Identity Manager

You can configure Oracle Access Manager to protect Oracle Identity Manager URLs.

2.4.1 Prerequisites

The prerequisites are as follows:

1. Ensure that the components required for the integration have been installed:
   - Oracle WebLogic Server

- Oracle Identity Navigator
- Oracle Access Manager
- Oracle Identity Manager

Note: Oracle Access Manager may be installed before Oracle Identity Manager and other IdM components, or it may be installed at the same time as other components.

See Also: *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*

2. Ensure that the following servers are running:
   - Oracle WebLogic Server
   - Oracle Access Manager Administration Server
   - Oracle Access Manager and Oracle Identity Manager managed servers

2.4.2 Configuration

For implementation details, see *Configuring Single Sign-on for Administration Consoles* in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

2.5 Integrating with Oracle Adaptive Access Manager for Native Authentication

In the native integration, Oracle Access Manager leverages Oracle Adaptive Access Manager to provide pre-and post-authentication services for Oracle Access Manager logins.

For details, see Section 6.2, "Oracle Access Manager-Oracle Adaptive Access Manager Basic Integration".

2.6 Enabling Single Sign-On for Oracle Identity Navigator

Oracle Identity Navigator provides an administrative portal to Oracle Identity Management components.

You can protect the Oracle Identity Navigator URL by SSO-enabling the Oracle Identity Navigator Administration Console using the WNA authentication scheme.

For integration details, see Chapter 3, "Integrating with Oracle Identity Navigator".

2.7 Integrating Oracle Access Manager with Oracle Identity Federation

You can configure Oracle Access Manager as an authentication engine for Oracle Identity Federation.

For integration details, see Chapter 4, "Integrating Oracle Identity Federation".

2.8 Integrating Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive Access Manager

This section describes various identity and password administration scenarios supported through IdM integration, and the processing flow for each integration.

For the integration procedure, see Chapter 7, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager".

2.8.1 Introduction and Benefits

This section provides an overview of integration of Oracle Access Manager with Oracle Identity Manager and Oracle Adaptive Access Manager.

2.8.1.1 How Oracle Access Manager Leverages Oracle Identity Manager and Oracle Adaptive Access Manager

In 11g Release 1 (11.1.1), Oracle Access Manager does not provide its own identity service; instead, Oracle Access Manager:

- consumes identity services provided by Oracle Identity Manager, LDAP directories, and other sources; and
- integrates with Oracle Identity Manager and Oracle Adaptive Access Manager to deliver a range of secure password collection functionality to Oracle Access Manager protected applications.

2.8.1.2 Benefits of the Integration

In the three-way Oracle Access Manager/Oracle Identity Manager/Oracle Adaptive Access Manager, the secure password collection features of the last two products are added to Oracle Access Manager-protected applications:

- Virtual authenticators to protect against phishing and perform secure credential collection;
- Fraud rules at various checkpoints to provide fraud detection and prevention by running fraud rules at various points;
- Knowledge Based Authentication (KBA) or One-Time Password (OTP) framework to provide additional authentication when needed; and
- Password management.

2.8.1.3 Dependency of Components in the Integration

The following components can be integrated separately:

- Oracle Access Manager and Oracle Adaptive Access Manager
- Oracle Identity Manager and Oracle Adaptive Access Manager

However, note the following dependency:

- When integrating Oracle Access Manager and Oracle Adaptive Access Manager, it is not necessary to involve Oracle Identity Manager.
- When integrating Oracle Adaptive Access Manager and Oracle Identity Manager, it is also necessary to integrate with Oracle Access Manager.

2.8.2 Deployment Options for Strong Authentication

The combination of Oracle Access Manager and Oracle Adaptive Access Manager enables fine control over the authentication process and provides full capabilities of pre- and post-authentication checking against Oracle Adaptive Access Manager policies.

In the context of this integration, Oracle Access Manager acts as the authenticating and authorizing module, while Oracle Adaptive Access Manager provides strong authenticators and performs the risk and fraud analysis.

2.8.2.1 About Native and Advanced Integration

There are two ways that Oracle Access Manager can leverage the strong authentication capabilities of Oracle Adaptive Access Manager:

- Native Integration with Oracle Adaptive Access Manager

  Oracle Access Manager users wishing to add basic login security, including Knowledge Based Authentication (KBA), may use the native integration option. This option does not require you to deploy a separate Oracle Adaptive Access Manager server (the functionality is accessed through native Oracle Adaptive Access Manager calls), so the footprint is reduced.

  The native integration does not provide access to more advanced features such as One-Time Password (OTP) through SMS, email, voice, or IM. The native integration is not customizable beyond basic screen branding.

- Advanced Integration with Oracle Adaptive Access Manager

  This option provides advanced features and customization beyond that available with native integration. Leveraging the Java Napp library, the integration of Oracle Access Manager and Oracle Adaptive Access Manager requires a full Oracle Adaptive Access Manager deployment.

For implementation details, see Chapter 6, "Integrating Oracle Access Manager and Oracle Adaptive Access Manager".

2.8.2.2 Component Interactions

The flow of interactions between the components is as follows:

1. A user tries to access a resource protected by Oracle Access Manager.
2. The Oracle Access Manager WebGate intercepts the (unauthenticated) request and redirects the user to the Oracle Adaptive Access Manager server.
3. The Oracle Adaptive Access Manager Server presents the user with the Oracle Adaptive Access Manager username page.
4. The user submits his username on the Oracle Adaptive Access Manager username page.
5. Oracle Adaptive Access Manager fingerprints the user device and runs pre-authentication rules to determine if the user should be allowed to proceed to the Oracle Adaptive Access Manager password page.

   Device fingerprinting is a mechanism to recognize the devices a user logs in with, whether it is a desktop computer, laptop computer, PDA, cell phone, kiosk, or other Web-enabled device.
6. If the user is allowed to proceed, the virtual authentication device rules are run during the Authentication Pad checkpoint. These rules determine which virtual authenticator to display in the Oracle Adaptive Access Manager password page.

If the user has registered with Oracle Adaptive Access Manager, the Oracle Adaptive Access Manager Server displays the Oracle Adaptive Access Manager password page with either the personalized TextPad or KeyPad.

If the user has not registered, Oracle Adaptive Access Manager displays the Oracle Adaptive Access Manager password page with the Generic TextPad.

7. The user submits his password on the Oracle Adaptive Access Manager password page.
8. The credentials collected from Oracle Adaptive Access Manager are verified against the identity store. After validation on the Oracle Access Manager side, Oracle Adaptive Access Manager runs the post-authentication rules.
9. Oracle Adaptive Access Manager interacts with the user to establish identity to perform the desired action. Oracle Adaptive Access Manager determines the user's risk score and executes any actions (for example, KBA or OTP) or alerts that are specified in the policy.
10. If the user is not registered, he may be asked to go through registration, for example, using KBA or OTP.

    Registration is required depending on security requirements, which specify whether the registration is mandatory or optional.
11. If authentication is successful and the user has the appropriate profile registered, Oracle Adaptive Access Manager sets the Oracle Access Manager cookie and redirects the user to the redirect URL.

2.8.3 Deployment Options for Password Management

You can implement password management features for Oracle Access Manager-protected applications by integrating Oracle Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager.

This section explains the deployment options. The next section, Section 2.8.4, "Password Management Scenarios", describes the scenarios that are supported by each deployment, and the flow that achieves each scenario.

In the context of password management, Oracle Access Manager works in two different deployment modes:

1. Oracle Access Manager and Oracle Identity Manager integrated for authentication and password management.

   For details, see Oracle Access Manager Integrated with Oracle Identity Manager
2. Oracle Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager integrated for authentication, password management, fraud detection and additional capabilities.

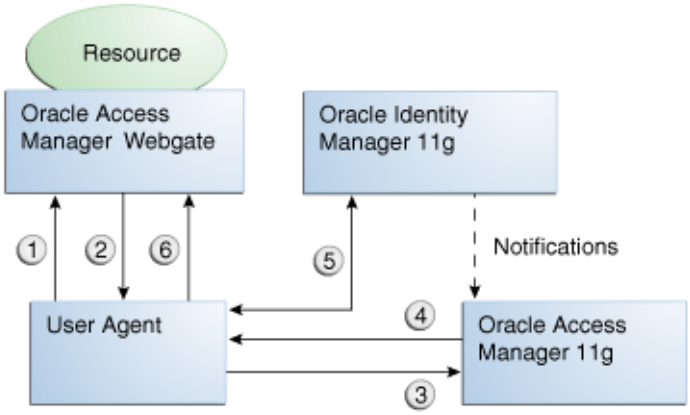
   For details of the processing flow, see Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager Integrated.

   For implementation details, see Chapter 7, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager".

2.8.3.1 Oracle Access Manager Integrated with Oracle Identity Manager

Figure 2–1 shows how password management is achieved when Oracle Access Manager and Oracle Identity Manager are integrated.

Figure 2–1 Integrating Oracle Access Manager and Oracle Identity Manager for Password Management



The flow of interactions between the components is as follows:

1. A user tries to access a resource protected by Oracle Access Manager.
2. The Oracle Access Manager WebGate intercepts the (unauthenticated) request.
3. WebGate redirects the user to the Oracle Access Manager login service, which performs validation checks.
4. If Oracle Access Manager finds any password management trigger conditions, such as password expiry, it redirects users to Oracle Identity Manager.
5. Oracle Identity Manager interacts with the user to establish the user's identity and carry out the appropriate action, such as resetting the password.
6. Oracle Access Manager logs the user in by means of auto-login, and redirects the user to the OAM-protected resource which the user was trying to access in Step 1.

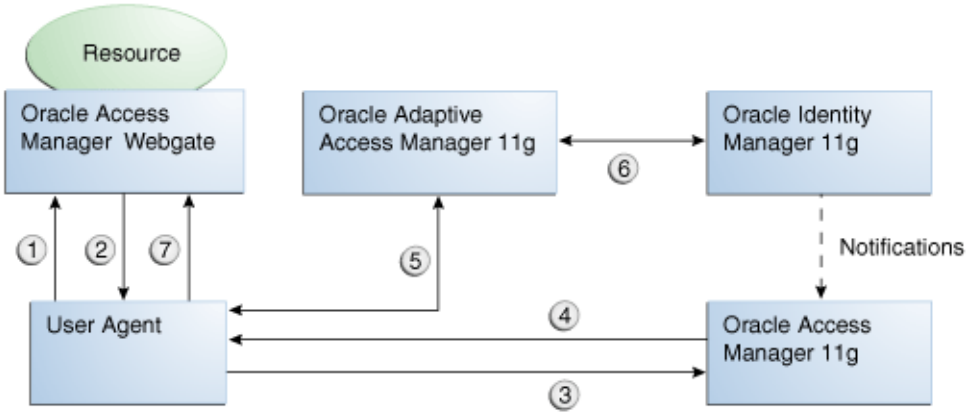
2.8.3.2 Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager Integrated

The integration between Oracle Adaptive Access Manager and Oracle Identity Manager allows the Oracle Adaptive Access Manager challenge questions to be used, at the same time using Oracle Identity Manager for password validation, storage and propagation.This integration leverages:

- Oracle Adaptive Access Manager for fraud prevention
- Oracle Access Manager password propagation to targets.

Figure 2–2 shows how password management is achieved when Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager are integrated.

Figure 2–2 Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager for Password Management



The flow of interactions between the components is as follows:

1. A user tries to access a resource protected by Oracle Access Manager.
2. The Oracle Access Manager WebGate intercepts the (unauthenticated) request and redirects the user login service, which presents the user with the Oracle Adaptive Access Manager username page.
3. The user is redirected to the Oracle Access Manager server. After validation,
4. The server checks if any password management triggering conditions are in effect. If a trigger condition (say, an expired password) is found, the Oracle Access Manager login service redirects the user to the Oracle Adaptive Access Manager server.
5. Oracle Adaptive Access Manager interacts with the user to establish identity.

   Interaction with Oracle Adaptive Access Manager proceeds as follows:

   - Oracle Adaptive Access Manager fingerprints the user device (a desktop computer, laptop computer, PDA, cell phone, kiosk, or other web enabled device) and runs pre-authentication rules to determine if the user should be allowed to proceed to the Oracle Adaptive Access Manager password page.
   - If the user is allowed to proceed, the Oracle Adaptive Access Manager Server displays the Oracle Adaptive Access Manager password page with the strong authenticator specified by the virtual authentication device rules.
   - If the user forgets his password, he can use the "Forgot your password" link and go through the "Forgot Password" flow.
   - The user submits his password on the Oracle Adaptive Access Manager password page.
   - Oracle Access Manager verifies the credentials collected from Oracle Adaptive Access Manager against the identity store. After validation by Oracle Access Manager, Oracle Adaptive Access Manager will run the post-authentication rules.
   - Oracle Adaptive Access Manager interacts with the user to establish identity in order to perform the desired action. Oracle Adaptive Access Manager determines the user's risk score and executes any actions (for example, KBA or OTP) or alerts that are specified in the policy.

- An unregistered user is asked to go through registration (Challenge Registration Flow), for example, KBA or OTP profile registration.

6. During credential processing, Oracle Adaptive Access Manager retrieves the password syntax and lifecycle policies from Oracle Identity Manager. Oracle Adaptive Access Manager enforces these policies while processing the trigger action.

   After the operation is complete, Oracle Adaptive Access Manager notifies Oracle Access Manager through a back channel.

7. Oracle Adaptive Access Manager auto-logs the user into Oracle Access Manager and redirects the user to the Oracle Access Manager-protected resource in step 1, using an authenticated request.

2.8.4 Password Management Scenarios

Common management scenarios supported by these deployment modes include:

- Self-Registration
- Password Change
- Forgot Password
- Account Lock and Unlock
- Challenge Setup
- Challenge Reset

2.8.4.1 Self-Registration

In this scenario, the user does not have an account but tries to access an Oracle Access Manager -protected resource. An Oracle Access Manager 11*g* Webgate intercepts the request, detects that the user is not authenticated, and redirects the user to the Oracle Access Manager Credential Collector (or 10*g* authenticating webgate), which shows the Oracle Access Manager Login page containing a "Register New Account" link.

On selecting this link, the user is securely redirected to Oracle Identity Manager Self Registration URL. Oracle Identity Manager interacts with the user to provision his account.

Self-Registration Flow

The Welcome Page is an unprotected page from which the self-registration/account creation can be initiated. This page contains two links, in addition to any introductory text or branding information. The links are:

- Register New Account - This is an unprotected URL to the corresponding application's registration wizard
- Login - This is a protected URL which serves as the landing page to which the user is directed after successfully completing the login.

Note: Any application protected by a single sign-on system with the self-registration requirement is expected to support a landing page. The options are:

- Self-registration using the link on the Oracle Access Manager login page.

  This is the most common option and is covered here.

- Self-registration using anonymous pages in other applications.

  If the application dictates that the user be automatically logged in at the end of the registration process, it can implement this by using the Oracle Platform Security Services APIs.

See Also: *Oracle Fusion Middleware Security Overview* for more information about Oracle Platform Security Services.

The account creation flow is as follows:

1. The user (using his browser) accesses the application's welcome page, which contains a **Register New Account** link.
2. The user clicks the **Register New Account** link, which takes the user to a custom self-registration page provided by the application.
3. The user interacts with the application to self-register.
4. On completion, the application performs an auto-login for the user.

The protected application is expected to send an SPML request to Oracle Identity Manager to create the user. After this, the application could choose to do one of the following:

- The application may choose not to auto-login the user. The application redirects the user to the protected landing page URL. Oracle Access Manager then shows the login page and takes the user through the login flow.
- If there is no approval associated with the request, the application can make use of the Oracle Platform Security Services (OPSS) APIs to conduct an auto-login to the specific landing page URL and respond with a redirect request with that URL (along with the SSO cookie). This takes the user directly to the landing page without bringing up the login page.
- Auto-login cannot be done if approval is needed. The application determines which profile to use at the time of SPML request. The application needs to respond with an appropriate page indicating that the request has been submitted.

2.8.4.2 Password Change

The Change Password flow enables users to change their password.

Password Change Flow with Oracle Access Manager and Oracle Identity Manager

In this situation, the user successfully logs into Oracle Access Manager but is required to immediately change the password. The user is not authorized to access protected resources until the password is changed and challenges have been set up.

On successful login, Oracle Access Manager detects if the triggering condition is in effect and redirects the user to the Oracle Identity Manager "Change Password" URL.

Oracle Identity Manager facilitates the user password change or challenge set-up and resets the triggering condition.

On completion, Oracle Identity Manager redirects the user to the protected resource.

This situation is triggered in the following cases:

- The "Change Password upon Login" flag is on. This occurs:
  - when a new user is created
  - when the administrator resets a user's password
- The password has expired.

This flow describes the situation where a user logs in to an Oracle Access Manager-protected application for the first time, and is required to change password before proceeding.

The following describes the Change Password flow:

1. Using a browser, the user tries to access an application URL that is protected by Oracle Access Manager.
2. Oracle Access Manager Webgate (SSO Agent) intercepts the request and redirects the user to the Oracle Access Manager Login Page.
3. The user submits credentials, which are validated by Oracle Access Manager.
4. Oracle Access Manager next determines if any of the First Login trigger conditions are valid. If so, Oracle Access Manager redirects the user to the Oracle Identity Manager Change Password URL.
5. Oracle Access Manager Webgate (SSO Agent) intercepts the request, determines that Oracle Identity Manager is protected by the Anonymous Authentication Policy, and allows the user request to proceed.
6. Oracle Identity Manager interacts with the user to enable the user to change his password. On completion, Oracle Identity Manager updates the attributes that triggered the First Login flow. Oracle Identity Manager then performs a user auto-login.
7. Oracle Identity Manager notifies Oracle Access Manager of the successful first login.
8. Oracle Identity Manager redirects the user to the application URL the user tried to access in step 1.

Password Change Flow - Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager Integrated

In this scenario, the user is at the Oracle Adaptive Access Manager password page and clicks the "Change your Password" link.

1. Using a browser, the user tries to access an application URL that is protected by Oracle Access Manager.
2. Oracle Access Manager WebGate intercepts the (unauthenticated) request.
3. Oracle Access Manager WebGate redirects the user to the Oracle Adaptive Access Manager Server and passes a redirect URL.
4. The Oracle Adaptive Access Manager Server presents the user with the Oracle Adaptive Access Manager username page.

5. The user submits his username on the Oracle Adaptive Access Manager username page.
6. Oracle Adaptive Access Manager fingerprints the user device (a desktop computer, laptop computer, PDA, cell phone, kiosk, or other web enabled device) and runs pre-authentication rules to determine if the user should be allowed to proceed to the Oracle Adaptive Access Manager password page.
7. If the user is allowed to proceed, the Oracle Adaptive Access Manager Server displays the Oracle Adaptive Access Manager password page with the strong authenticator specified by the virtual authentication device rules.
8. The user submits his password on the Oracle Adaptive Access Manager password page.
9. During authentication, Oracle Adaptive Access Manager calls the Oracle Access Manager Java APIs to validate the credentials.
10. If authentication is successful and the user has registered questions, but he wants to reset his password, the user clicks the Change Password link.
11. The user is redirected to the Change Password URL of Oracle Adaptive Access Manager, which allows the users to change his password.
12. Oracle Adaptive Access Manager collects the current password and the new password, and confirms the password from the user using its authenticators.
13. Password policy information, obtained from Oracle Identity Manager, is displayed to guide the user to select the appropriate password.
14. Oracle Adaptive Access Manager makes Oracle Identity Manager calls to update the password in the repository.
15. If the update is successful, Oracle Adaptive Access Manager redirects the user to the resource protected by Oracle Access Manager.

2.8.4.3 Forgot Password

The Forgot Password flow allows users to reset their password after successfully answering all challenge questions.

Forgot Password Flow for Oracle Access Manager/Oracle Identity Manager Integration

In this scenario, the user is at the Oracle Access Manager Login page and clicks the "Forgot Password" link. Oracle Access Manager redirects the user to the Oracle Identity Manager "Forgot Password" URL, and passes the destination URL to which Oracle Identity Manager must redirect upon a successful password change as a query parameter (`backURL`).

Oracle Identity Manager asks the user the challenge questions. Upon providing the correct responses, the user is allowed to specify a new password.

On completion, Oracle Identity Manager redirects the user to the protected resource.

The Forgot Password flow is as follows:

1. Using a browser, the user tries to access an application URL that is protected by Oracle Access Manager.
2. The Oracle Access Manager Webgate (SSO Agent) intercepts the request and redirects the user to the Oracle Access Manager Login Page.

3. The user clicks on the Forgot Password link on the Oracle Access Manager Login page, which sends the user to the Oracle Identity Manager Forgot Password URL.
4. Oracle Identity Manager interacts with the user to enable the user to reset the password. On completion, Oracle Identity Manager performs a user auto-login.
5. Oracle Identity Manager redirects the user to the application URL to which access was attempted in step 1.

Forgot Password Flow for Oracle Access Manager/Oracle Identity Manager/Oracle Adaptive Access Manager Integration

With Oracle Adaptive Access Manager and Oracle Identity Manager integration, the forgot password feature is made available as a link from the Oracle Adaptive Access Manager password page. The flow starts when the user is at the Oracle Adaptive Access Manager password page and clicks the "Forgot your password" link.

The flow is as follows:

1. Using a browser, the user tries to access an application URL that is protected by Oracle Access Manager.
2. Oracle Access Manager WebGate intercepts the (unauthenticated) request.
3. Oracle Access Manager WebGate redirects the user to the Oracle Adaptive Access Manager Server.
4. The Oracle Adaptive Access Manager Server presents the user with the Oracle Adaptive Access Manager username page.
5. The user submits his username on the Oracle Adaptive Access Manager username page.
6. Oracle Adaptive Access Manager fingerprints the user device (a desktop computer, laptop computer, PDA, cell phone, kiosk, or other web enabled device) and runs pre-authentication rules to determine if the user should be allowed to proceed to the Oracle Adaptive Access Manager password page.
7. If the user is allowed to proceed, the Oracle Adaptive Access Manager Server displays the Oracle Adaptive Access Manager password page with the strong authenticator specified by the virtual authentication device rules.
8. The user clicks the "Forgot your password" link on the Oracle Adaptive Access Manager password page.
9. Oracle Adaptive Access Manager presents the user with a pre-registered set of challenge questions.
10. The user provides the answers to the challenge questions.
11. Oracle Adaptive Access Manager uses fuzzy logic to validate the answers to challenge questions.
12. If the user provided correct responses, he is redirected to the Password Reset page.
13. Password policy text from Oracle Identity Manager is retrieved by Oracle Adaptive Access Manager by making calls to Oracle Identity Manager, and then shown in the Reset Password page.
14. The user enters the new password.
15. Oracle Adaptive Access Manager calls Oracle Identity Manager to update the repository with the new password.

16. If the update is successful, Oracle Adaptive Access Manager redirects the user to the resource protected by Oracle Access Manager.

2.8.4.4 Account Lock and Unlock

Oracle Access Manager keeps track of login attempts and locks the account when the count exceeds the established limit.

When an account is locked, Oracle Access Manager displays the Help Desk contact information.

When contacted by the end user, the Help Desk unlocks the account using the Oracle Identity Manager administrative console. Oracle Identity Manager then notifies Oracle Access Manager about the changes.

Account Lock and Unlock Flow

When the number of unsuccessful user login attempts exceeds the value specified in the password policy, the user account is locked. Any login attempt after the user account has been locked displays a page that provides information about the account unlocking process, which will need to be customized to reflect the process (Help Desk information or similar) that is followed by your organization.

The following describes the account locking/unlocking flow:

1. Using a browser, a user tries to access an application URL that is protected by Oracle Access Manager.
2. Oracle Access Manager Webgate (SSO Agent) intercepts the request and redirects the user to the Oracle Access Manager login page.
3. The user submits credentials that fail Oracle Access Manager validation. Oracle Access Manager renders the login page and asks the user to resubmit his or her credentials.
4. The user's unsuccessful login attempts exceed the limit specified by the policy. Oracle Access Manager locks the user account and redirects the user to the Oracle Access Manager Account Lockout URL, which displays help desk contact information.
5. The user contacts the help desk over the telephone and asks an administrator to unlock the account.
6. Oracle Identity Manager notifies Oracle Access Manager of the account unlock event.
7. The user attempts to access an application URL and this event triggers the normal Oracle Access Manager single sign-on flow.

2.8.4.5 Challenge Setup

The Challenge Setup enables users to register challenge questions and answers.

Challenge Setup Flow for Oracle Access Manager-Oracle Identity Manager Integration

Oracle Access Manager detects and redirects on password trigger conditions:

- Password Policy is updated to increase the required number of challenges.
- Password Policy is updated to require challenges.

When such redirection happens, Oracle Identity Manager checks if the challenge questions are set. If not, it asks the user to set up challenge questions in addition to resetting the password.

The following describes the flow:

> **Note:** The flow assumes First Login is not required.

1. Using a browser, the user tries to access an application URL that is protected by Oracle Access Manager.
2. Oracle Access Manager Webgate (SSO agent) intercepts the request and redirects the user to the Oracle Access Manager Login Page.
3. The user submits credentials, which are validated by Oracle Access Manager. If a password triggering condition is detected, Oracle Access Manager redirects the user to the Oracle Identity Manager change password URL.
4. The Oracle Access Manager Webgate (SSO agent) intercepts the request, determines that Oracle Identity Manager is protected by the anonymous authentication policy, and allows the user request to proceed.
5. Oracle Identity Manager interacts with the user to set up the challenges. On completion, Oracle Identity Manager updates the attributes that triggered the set challenges flow.
6. Oracle Identity Manager redirects the user to the application URL that the user attempted to access in Step 1.

Challenge Setup Flow for Oracle Access Manager-Oracle Identity Manager-Oracle Adaptive Access Manager Integration

In this scenario, the user is successfully authenticated but is required to register challenge questions. The user is not authorized to access protected resources until the challenges questions have been registered.

> **Note:** When adding Oracle Adaptive Access Manager to existing Oracle Identity Manager deployments, you will need to forego all the existing questions and answers that are registered in Oracle Identity Manager. Instead, users are asked to register the challenge questions again in Oracle Adaptive Access Manager on the next login.

1. Using a browser, the user tries to access an application URL that is protected by Oracle Access Manager.
2. Oracle Access Manager WebGate intercepts the (unauthenticated) request.
3. Oracle Access Manager WebGate redirects the user to the Oracle Adaptive Access Manager Server and passes a redirect URL.
4. Oracle Adaptive Access Manager presents the user with the Oracle Adaptive Access Manager username page.
5. The user submits his username on the Oracle Adaptive Access Manager username page.
6. Oracle Adaptive Access Manager fingerprints the user device (a desktop computer, laptop computer, PDA, cell phone, kiosk, or other web enabled device)

and runs pre-authentication rules to determine if the user should be allowed to proceed to the Oracle Adaptive Access Manager password page.

7. If the user is allowed to proceed, the Oracle Adaptive Access Manager Server displays the Oracle Adaptive Access Manager password page with the strong authenticator specified by the virtual authentication device rules.
8. The user submits his password on the Oracle Adaptive Access Manager password page.
9. During authentication, Oracle Adaptive Access Manager calls Oracle Access Manager to validate the credentials.
10. After authentication, Oracle Adaptive Access Manager checks if the user has registered challenge questions.
11. If the user has not registered for challenges, Oracle Adaptive Access Manager interacts with the user to set up the challenges (select challenge questions and register answers and/or set up an OTP profile).
12. If the registration is successful Oracle Adaptive Access Manager redirects the user to the Oracle Access Manager protected resource.

2.8.4.6 Challenge Reset

Challenge Reset enables users to reset their challenge registration. This feature is available when Oracle Access Manager is integrated with Oracle Adaptive Access Manager.

The flow is as follows:

1. Using a browser, the user tries to access an application URL that is protected by Oracle Access Manager.
2. Oracle Access Manager WebGate intercepts the (unauthenticated) request.
3. Oracle Access Manager WebGate redirects the user to the Oracle Adaptive Access Manager Server and passes a redirect URL.
4. The Oracle Adaptive Access Manager Server presents the user with the Oracle Adaptive Access Manager username page.
5. The user submits his username on the Oracle Adaptive Access Manager username page.
6. Oracle Adaptive Access Manager fingerprints the user device (a desktop computer, laptop computer, PDA, cell phone, kiosk, or other web enabled device) and runs pre-authentication rules to determine if the user should be allowed to proceed to the Oracle Adaptive Access Manager password page.
7. If the user is allowed to proceed, the Oracle Adaptive Access Manager Server displays the Oracle Adaptive Access Manager password page with the strong authenticator specified by the virtual authentication device rules.
8. The user submits his password on the Oracle Adaptive Access Manager password page.
9. During authentication, Oracle Adaptive Access Manager calls Oracle Access Manager to validate the credentials.
10. If authentication is successful and the user has questions registered, but he wants to reset his challenge questions, the user clicks the Reset Challenge link.
11. The user is redirected to Oracle Adaptive Access Manager where he can reset challenge questions.

12. After resetting the challenge registration, Oracle Adaptive Access Manager prompts the user to register for challenge.
13. If the user did not complete the registration, they are prompted for registration on the next login.

3

Integrating with Oracle Identity Navigator

This chapter describes how Oracle Access Manager integrates with Oracle Identity Navigator.

Using the procedure described in this chapter, you can protect Oracle Identity Navigator with Oracle Access Manager using a WebGate agent.

The procedure uses an Oracle Internet Directory authenticator to enable Oracle WebLogic Server to assert the subject set by Oracle Access Manager.

> **Note:** This is a specific example of Oracle Access Manager used to protect URLs. Although it outlines the general approach for this type of configuration, you are not limited to using the exact steps and components used here. For example, Oracle Internet Directory is one of several identity stores certified with Oracle Access Manager 11*g*.

> **Note:** In Release 11.1.1.5.0, Oracle Identity Navigator is protected by the domain agent out-of-the-box. In earlier releases, this was not the case; manual configuration was required to protected the URLs.

This chapter contains this section:

3.1 Enabling Single Sign-On

You can use Oracle Access Manager to SSO-enable the Oracle Identity Navigator Administration Console using the Kerberos authentication scheme with Windows Native Authentication (WNA) as the challenge method.

The prerequisites are as follows:

- Oracle HTTP Server has been installed.

  When installing Oracle HTTP Server, uncheck Oracle WebCache and associated selected components with WebLogic domain.
- Oracle Access Manager 11*g* has been installed and configured properly.
- Oracle HTTP Server 11g has been installed and configured as a front-ending proxy web server for Oracle Identity Navigator.
- Oracle Access Manager 11g webgate for Oracle HTTP Server 11g has been installed on the Oracle HTTP Server 11g.

See Also: *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* for details about installation of the listed components. The following sections are of specific interest:

- Installing and Configuring Only Oracle Identity Navigator
- Installing and Configuring Only Oracle Access Manager

The high-level SSO-enablement steps are as follows:

- Use the Oracle Access Manager Administration Console to configure a new resource for the agent under which the Oracle Identity Navigator URL is to be protected.
- Configure Oracle HTTP Server to point to the Oracle Access Manager domain which has the resources and policies configured.
- Use the Administration Console to add the two new identity providers, namely the Oracle Access Manager Identity Asserter and the Oracle Internet Directory Authenticator.
- Use Oracle Directory Services Manager (ODSM) to grant administrator privileges to the login user.

These steps are detailed in subsequent sub-sections.

3.1.1 Configure a New Resource for the Agent

At the Oracle Access Manager console:

1. Select the **Policy Configuration** tab.
2. Under **Application Domains**, select the agent under which the Oracle Identity Navigator URL is to be protected (for example, -OIMDomain).
3. Choose **Resources** and click the **create** icon to add a new resource. Enter the type, host identifier and value, (/oinav/…/*) and click the **Apply** button.
4. Choose Protected Policy or the policy whose authentication schema is the LDAP schema. In the resources table, click the **add** icon and choose the Oracle Identity Navigator URL (/oinav/…/*) from the drop-down list.
5. Repeat the step for Authorization Policy.

3.1.2 Configure Oracle HTTP Server for the Oracle Access Manager Domain

Take these steps to ensure that Oracle HTTP Server points to the Oracle Access Manager domain where the resources and policies are configured:

1. Navigate to the Oracle HTTP Server server config directory, for example, `/scratch/mydir1/oracle/product/11.1.1/as_1/instances/instance1/config/OHS/ohs1`), and find the `mod_wl_ohs.conf` file.
2. In the `<IfModule mod_weblogic.c>` block, add the host and the port number of the Oracle Identity Navigator URL to be protected. For example:

   ```
   MatchExpression /oinav* WebLogicHost=host WebLogicPort=port
   ```

3. Restart the Oracle HTTP Server server in the OHS install `bin` directory, for example, `/scratch/mydir1/oracle/product/11.1.1/as_1/instances/instance1/bin`) by executing the following command:

```
-./opmnctl restartproc ias=component=ohs1
```

3.1.3 Add New Identity Providers

Take these steps to add two new identity providers and grant administrator privileges to the login user:

1. Using the Administration Console, navigate to **Security Realms**, then **myreleam**, then **Providers**.
2. Add these two providers: OAM Identity Asserter and OID Authenticator.
3. Set the Control Flag of the OAM Identity Asserter to `Required`
4. Update the following settings in the OID Authenticator:
   - Set the Control Flag to `Sufficient`
   - Select the **Provider specific** tab and make the necessary changes, supplying the host, port, and other credentials of the Oracle Internet Directory server. Configure the correct LDAP setting in the OID Authenticator.

   The users and Groups in the LDAP will be reflected in the console.
5. Use Oracle Directory Services Manager (ODSM) to give the administrator privilege to the login user:
   a. Create a user in the LDAP server that is associated with Oracle Access Manager, for example:
   `uid=testuser,cn=users,dc=us,dc=oracle,dc=com`
   b. Create an Administrators group in the LDAP directory, namely
   `cn=Administrators,cn=groups,dc=us,dc=oracle,dc=com`
   c. Assign the Administrators role to the user, `testuser`, by adding the user to the Administrator group.
   d. You can now test an SSO by this user to Oracle Identity Navigator.
6. Re-order the providers as follows:
   a. OAMIdentityAsserter
   b. Authenticator
   c. Default Authenticator
   d. Default Identity Asserter
7. Restart Oracle WebLogic Server.
8. Enter the protected Oracle Identity Navigator URL, which will have the host and port from the Oracle HTTP Server install:

   `http://`*`OHSHost:OHSPort`*`/oinav/faces/idmNag.jspx`

4

Integrating Oracle Identity Federation

This chapter describes how to integrate Oracle Access Manager with Oracle Identity Federation to create an authenticated session.

This chapter contains these sections:

4.1 Background and Integration Overview

This section provides background about the integration procedure. Topics include:

4.1.1 About Integration with Oracle Identity Federation

About Oracle Identity Federation

Oracle Identity Federation is a standalone, self-contained federation server that enables single sign-on and authentication in a multiple-domain identity network.

The SP integration Engine included with Oracle Identity Federation consists of a servlet that processes requests from the server to create a user authenticated session at the Identity and Access Management (IAM) server. The engine includes several internal plug-ins that allow it to interact with different IAM servers, including Oracle Access Manager.

About the Integration

Two integration modes are described in this chapter:

- SP Mode

This mode enables Oracle Identity Federation to authenticate the user and propagate the authentication state to Oracle Access Manager, which maintains the session information.

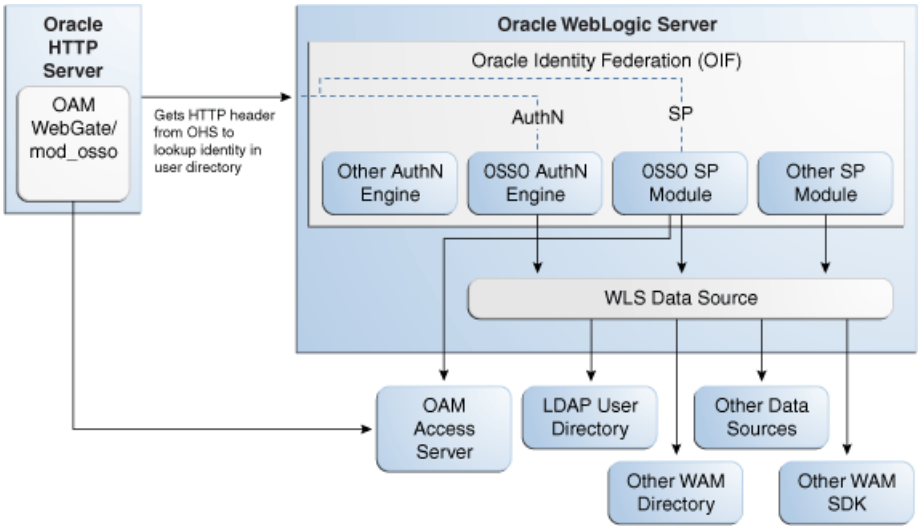
- Authentication Mode

  This mode enables Oracle Access Manager to authenticate the user.

> **Note:** When integrating in Authentication Mode, SP Mode will be required for logout purposes.

Figure 4–1 describes the processing flow in each mode.

Figure 4–1 Oracle Access Manager and Oracle Identity Federation



In the SP mode, Oracle Identity Federation uses the federation protocols to identify a user, and requests the authentication module to create an authenticated session at Oracle Access Manager. To integrate in SP mode, see "SP Mode Integration Procedure".

In the authentication mode, Oracle Access Manager looks up the user identity in the LDAP store and obtains a session cookie so that the user can access the requested resource, which is protected by either mod_osso or Oracle Access Manager 11*g* WebGate. To integrate in authentication mode, see "Authentication Mode Integration Procedure".

4.1.2 Overview of Integration Tasks

The tasks required to integrate Oracle Access Manager with Oracle Identity Federation are similar for both modes, with some variation.

SP Mode Integration Procedure

Configuring the SP mode requires the following tasks:

1. Ensure that the necessary components, including Oracle WebLogic Server and Identity Management (IdM) components, are installed and operational.

   For details, see Section 4.1.3 and Section 4.1.4.

2. Register Oracle HTTP Server as a partner with Oracle Access Manager to protect a resource.

   For details, see Section 4.2.

3. Configure the Oracle Identity Federation server to function as a service provider (SP) with Oracle Access Manager.

   For details, see Section 4.3.

4. Configure the Oracle Access Manager server to delegate the authentication to Oracle Identity Federation.

   For details, see Section 4.4.

5. Protect the resource with the OIFScheme.

   For details, see Section 4.5.

6. Test the integration.

   For details, see Section 4.6.

Authentication Mode Integration Procedure

Configuring the authentication mode requires the following tasks:

1. Ensure that the necessary components, including Oracle WebLogic Server and Identity Management (IdM) components, are installed and operational.

   For details, see Section 4.1.3 and Section 4.1.4.

2. Register Oracle HTTP Server as a partner with the Oracle Access Manager server to protect a resource.

   For details, see Section 4.2.

3. Configure the Oracle Identity Federation server to function as an identity provider (IdP) with Oracle Access Manager.

   For details, see Section 4.3.

4. Test the integration.

   For details, see Section 4.6.

4.1.3 Prerequisites

You must install the following components prior to undertaking the integration tasks:

- Oracle WebLogic Server
- Oracle HTTP Server 11*g*
- Oracle Access Manager 11*g*
- Oracle Identity Federation 11*g*
- mod_osso (required in authentication mode)

Note: Refer to the Certification Matrix for platform and version details.

See Also: *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*

4.1.4 Additional Setup

Oracle WebLogic Server

Ensure that the administration and managed servers are up and running.

Oracle HTTP Server

For testing purposes, identify or create a resource to be protected; for example, create an index.html file to serve as a test resource.

Oracle Identity Federation

Access the Fusion Middleware Control console for the Oracle Identity Federation server using a URL of the form:

`http://oif_host:oif_em_port/em`

Verify that all the servers are running.

4.2 Register Oracle HTTP Server with Oracle Access Manager

This section shows how you can register Oracle HTTP Server and either 11*g* WebGate or mod_osso with Oracle Access Manager, depending on the protection mechanism you have chosen.

This section contains these topics:

- Register Oracle HTTP Server and mod_osso with Oracle Access Manager
- Register Oracle HTTP Server and WebGate with Oracle Access Manager

4.2.1 Register Oracle HTTP Server and mod_osso with Oracle Access Manager

Follow these steps to register Oracle HTTP Server and mod_osso with Oracle Access Manager:

Note: MW_HOME represents the Oracle Fusion Middleware Home directory.

---

1. Locate the `OSSORequest.xml` file in the directory:

   `MW_HOME/Oracle_IDM1/oam/server/rreg/input`

   Make the necessary changes to the file by setting the host, port, and agent name to appropriate values. The server address is the Oracle Access Manager admin server address and AgentBaseURL must have the Oracle HTTP Server host and port.

2. Locate the `oamreg.sh` script, which resides in:

   `MW_HOME/Oracle_IDM1/oam/server/rreg/bin`

   Execute the script using this command string (user is `weblogic`, and you must supply the password):

   ```
   ./oamreg.sh inband input/OSSORequest.xml
   ```

3. Configure mod_osso with static directives. For instructions see "Configuring mod_osso with Static Directives" in the *Oracle Fusion Middleware Application Security Guide*.
4. The script executed in Step 3 generates an `osso.conf` file in the directory:

   `MW_HOME/Oracle_IDM1/oam/server/rreg/output/AgentName`

   Copy the file to the following location:

   `Oracle_WT1/instances/instance1/config/OHS/ohs1/moduleconf/osso/`

5. Locate the `mod_osso.conf` file in the directory:

   `Oracle_WT1/instances/instance1/config/OHS/ohs1/moduleconf`

   Add these directives to the file:

   ```
   OssoSecureCookies off
   OssoConfigFile path_to_osso.conf_file
   ```

6. Uncomment the `Location` tag and fill in the protected resource path.

   In authentication mode:

   ```
   <Location /fed/user/authnoam11g>
      require valid-user
      AuthType Osso
   </Location>
   ```

7. Restart Oracle HTTP Server.

   `Oracle_WT1/instances/instance1/bin/opmnctl restartproc process-type=OHS`

4.2.2 Register Oracle HTTP Server and WebGate with Oracle Access Manager

Integrating Oracle Access Manager 11*g* WebGate with Oracle Identity Federation requires:

- Integrating Oracle Identity Federation with Oracle Access Manager 11*g* in SP mode (as described in Section 4.3), using the OAM11g SP engine
- Enabling logout in the OAM11g SP engine: the logout integration with Oracle Access Manager 11g will be performed using the OAM11g SP engine, instead of the OAM11g authentication engine

Follow these steps to register Oracle HTTP Server andOracle Access Manager 11*g* WebGate with Oracle Access Manager for authentication:

> **Note:** In this procedure, `MW_HOME` represents the Oracle Fusion Middleware Home directory.

1. Locate the OAM11GRequest.xml file or the OAM11GRequest_short.xml file, which resides in the directory:

   `MW_HOME/Oracle_IDM1/oam/server/rreg/input`

   Make the necessary changes to the file.

2. Locate the oamreg.sh script, which resides in the directory:

   `MW_HOME/Oracle_IDM1/oam/server/rreg/bin`

Execute the script using the command string:

> **Note:** The user is `weblogic`, and you must supply the password.

```
./oamreg.sh inband input/OAM11GRequest.xml
```

or

```
./oamreg.sh inband input/OAM11GRequest_short.xml
```

3. Using the Oracle Access Manager console, create a resource representing the Oracle Identity Federation URL to be protected by Oracle Access Manager for authentication. This URL contains the hostname and port of the Oracle Identity Federation server, and the path to the resource, which is mode-dependent.

   For example, in authentication mode:

   `https://oif-host:oif-port/fed/user/authnoam11g`

4. Protect this resource with an authentication policy and an authorization policy.
5. Restart Oracle HTTP Server:

   ```
   Oracle_WT1/instances/instance1/bin/opmnctl restartproc process-type=OHS
   ```

4.3 Configuring Oracle Identity Federation for Oracle Access Manager

This section describes how to configure Oracle Identity Federation to be integrated with Oracle Access Manager:

- In SP mode, where Oracle Access Manager will delegate authentication to Oracle Identity Federation for Federation SSO.
- In Authentication mode, where Oracle Identity Federation will delegate authentication to Oracle Access Manager.

> **Note:** When integrating in Authentication Mode, SP Mode will be required for logout purposes.

This section contains these topics:

4.3.1 Verifying User Data

Oracle Identity Federation and Oracle Access Manager must use the same LDAP directory. The LDAP directory must be defined in Oracle Access Manager as the default Identity Store and in Oracle Identity Federation as the User Data Store. The following steps verify the data store configuration.

1. Locate the Oracle Identity Federation instance in Fusion Middleware Control.
2. Navigate to Administration, then Data Stores.

3. Ensure that the User Data Store points to the same directory as the default Access Manager Identity Store

4.3.2 Configuring the Oracle Identity Federation Authentication Engine

The following procedure configures the Oracle Identity Federation Authentication Engine to retrieve information provided by the WebGate 11g agent.

1. Locate the instance of Oracle Identity Federation in Fusion Middleware Control.
2. Navigate to Administration and then Authentication Engines.
3. Enable the Oracle Access Manager 11g authentication engine.
4. Select the Agent Type.
   - If mod_osso is used, select Mod OSSO as the Agent Type.
   - If WebGate 11g is used, select WebGate 11g as the Agent Type.
5. Select the User Unique ID Header.
   - If mod_osso is used, select Proxy Remote User as the User Unique ID Header.
   - If WebGate 11g is used, enter OAM_REMOTE_USER as the User Unique ID Header.
6. In the Default Authentication Engine drop-down list, select Oracle Access Manager 11g.
7. Logout configuration: leave logout disabled as it will be configured in the Oracle Access Manager 11g SP Engine
8. Click Apply.

4.3.3 Configuring the Oracle Identity Federation SP Integration Module

This section lists the steps that need to be performed to configure Oracle Identity Federation in SP mode for Access Manager, so that Oracle Identity Federation can send assertion tokens and direct session management to Access Manager.

1. Locate the instance of Oracle Identity Federation in Fusion Middleware Control.
2. Navigate to Administration and then Service Provider Integration Modules.
3. Select the Oracle Access Manager 11g tab.
4. Configure as follows then click Apply.
   - Check the Enable SP Module box.
   - Select Oracle Access Manager 11g from the Default SP Integration Module drop-down menu.
   - Check the Logout Enabled box.
   - Configure the Login URL as

     ```
     http://oam_host:oam_port/oam/server/dap/cred_submit
     ```

     where oam_host and oam_port are the host and port number of the Oracle Access Manager server respectively.
   - Configure the Logout URL as

     ```
     http://oam_host:oam_port/oam/server/logout
     ```

where oam_host and oam_port are the host and port number of the Oracle Access Manager server respectively.

- Set the value of the Username Attribute to `uid` to match the Oracle Access Manager username attribute.

5. Click Regenerate.

   This action generates a keystore file that contains the keys used to encrypt and decrypt tokens that are exchanged between the Oracle Access Manager and Oracle Identity Federation servers. Be sure to save the keystore file using the Save As dialog.

6. Copy the keystore file to a location within the installation directory of Access Manager.

   Make a note of the location to refer to later.

4.4 Configuring Oracle Access Manager for Oracle Identity Federation

This section describes how to configure Oracle Access Manager to integrate with Oracle Identity Federation.

- In SP mode, where Oracle Access Manager will delegate authentication to Oracle Identity Federation for Federation SSO.
- In Authentication mode, where Oracle Identity Federation will delegate authentication to Oracle Access Manager.

This section contains these topics:

4.4.1 Configuring the OIFScheme

The following procedure configures Oracle Access Manager to redirect the user to Oracle Identity Federation for authentication when the OIFScheme is used to protect a resource using Federation SSO.

1. Log in to the Oracle Access Manager Administration Console.
2. Select the Policy Configuration tab.
3. Select and open the OIFScheme.
4. In the Challenge URL field, modify the value of OIFHost and port to reflect your deployment.
5. Confirm that the value of the Context Type drop-down is set to `external`.
6. Click Apply to save the changes.

4.4.2 Registering Oracle Identity Federation as a Trusted Access Manager Partner

Use the WebLogic Scripting Tool and the following procedure to update the OIFDAP partner block in the `oam-config.xml` configuration file.

Note: Be sure you have copied the keystore file to a location within the installation directory of Access Manager. See Configuring the Oracle Identity Federation SP Integration Module.

1. Enter the shell environment by executing the WLST script.

   ```
   $DOMAIN_HOME/common/bin/wlst.sh
   ```

2. Connect to the Oracle Access Manager administration server using the following syntax.

   ```
   connect('weblogic','password','host:port')
   ```

3. Execute the following command to update the partner block in the configuration file.

   ```
   registerOIFDAPPartner(keystoreLocation=location_of_keystore_file,
    logoutURL=logoutURL)
   ```

   where logoutURL defines the Oracle Identity Federation logout URL to invoke when the Oracle Access Manager server logs the user out. For example:

   ```
   registerOIFDAPPartner(keystoreLocation="/home/pjones/keystore",
    logoutURL="http://abcdef0123.in.mycorp.com:1200/fed/
    user/spslooam11g?doneURL=
    http://abc1234567.in.mycorp.com:6001/oam/pages/logout.jsp")
   ```

4.4.3 Updating the MatchLDAPAttribute

MatchLDAPAttribute is used to locate the user in Oracle Access Manager in a Federation SSO SP flow. Use the following procedure to set the value to `uid` by modifying the `oam-config.xml` file.

1. Open the `oam-config.xml` file located in `$DOMAIN_HOME/config/fmwconfig/`.

2. Locate the `MatchLDAPAttribute` string (located under the DAPModules and 7DASE52D elements) and set the value to `uid`.

   The modified section should look as follows:

   ```
   <Setting Name="DAPModules" Type="htf:map">
    <Setting Name="7DASE52D" Type="htf:map">
    <Setting Name="name" Type="xsd:string">DAP</Setting>
    <Setting Name="MatchLDAPAttribute" Type="xsd:string">uid</Setting>
   <Setting Name="MAPPERCLASS" Type="xsd:string">oracle.security.am.engine.authn.
    internal.executor.DAPAttributeMapper</Setting>
   </Setting>
   </Setting>
   ```

3. Save the file and exit.

4.5 Protecting a Resource with OIFScheme

After the integration of Oracle Access Manager and Oracle Identity Federation in SP mode, a resource can now be protected using OIFScheme. OIFScheme triggers a Federation SSO operation when an unauthenticated user requests access to a resource protected by said scheme. To protect using the OIFScheme, in the applicable

Application Domain (under the Policy Configuration tab), define an Authentication Policy using the OIFScheme and protect a resource using that Authentication Policy.

4.6 Testing The Configuration

The final task is to test the configured integration. The steps are different depending on whether you have used SP Mode or Authentication Mode. More information is in the following sections.

- Testing With SP Mode
- Testing With Authentication Mode

4.6.1 Testing With SP Mode

Follow this procedure to test for correct configuration when in SP mode.

1. Establish Federated Trust between Oracle Identity Federation and a remote Identity Provider.
2. Set that Identity Provider as the Default SSO Identity Provider.
3. Access the protected resource.

   When set up correctly, you should be redirected to the Identity Provider for authentication.
4. Enter valid credentials on the login page.

   The user should exist in both the Identity Provider security domain and the Oracle Identity Federation and Oracle Access Manager security domains.
5. Check that you are redirected to the protected page.

   Additionally, verify that the following cookies have been created:

   - OAM_ID
   - ORA_OSFS_SESSION
   - OHS Cookie

4.6.2 Testing With Authentication Mode

Follow this procedure to test for correct configuration when in Authentication Mode.

1. Establish Federated Trust between Oracle Identity Federation and a remote Service Provider.
2. Initiate Federation SSO from the Service Provider.
3. Verify that you are redirected to the Oracle Access Manager login page at the Identity Provider.
4. Enter valid credentials and process the page.
5. Verify that you are redirected to the Service Provider domain.

5

Integrating Oracle Access Manager and Oracle Identity Manager

This chapter explains how to integrate Oracle Access Manager with Oracle Identity Manager.

The instructions in this chapter use Oracle Internet Directory as an example directory server only. Refer to the system requirements and certification documentation on Oracle Technology Network for more information about supported configurations. For more information, see Section 1.4, "System Requirements and Certification."

If using a different directory server in your environment, you will need to modify the steps accordingly. You can refer to the configuration scenarios described in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management* for more information.

This chapter contains these sections:

5.1 About the Integration

This integration enables you to manage identities with Oracle Identity Manager and control access to resources with Oracle Access Manager.

For more information, see Section 2.3, "Enabling Identity Administration with Oracle Identity Manager".

The high-level integration tasks consist of:

- Ensuring that all prerequisites to integration have been met
- Configuring the Oracle Access Manager server to integrate with Oracle Identity Manager
- Creating the administrative user in the directory server
- Configuring the Oracle Identity Manager server to integrate with Oracle Access Manager

- Verifying the integration.

Perform the tasks in order, from Section 5.2 through Section 5.5.

5.2 Prerequisites

Take the following steps to prepare for the integration procedure:

1. Install and configure required components, which include:
   - Oracle Database
   - Directory server (Oracle Internet Directory used as an example)
   - Oracle WebLogic Server
   - WebLogic domain with 11*g* components:
     - Oracle Access Manager
     - Oracle Identity Manager
     - Oracle SOA Suite

     See Also: *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*

2. Set the environment variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME` and `ORACLE_HOME`.

   Set `IDM_HOME` to `IDM_ORACLE_HOME`, where Oracle Internet Directory is installed.

   Set `ORACLE_HOME` to `IAM_ORACLE_HOME`, where Oracle Access Manager and Oracle Identity Manager are installed.

3. Locate the `idmConfigTool` utility in the directory:

   IAM_ORACLE_HOME`/idmtools/bin`

   You will use this utility in the next few steps to get the identity store ready for the integration.

4. Create a properties file with contents similar to the following:

```
IDSTORE_HOST : idstore.mycompany.com
IDSTORE_PORT : 389
IDSTORE_BINDDN : cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=mycompany,dc=com
```

   where:

   - IDSTORE_HOST and IDSTORE_PORT are the host and port, respectively, of your identity store directory. If you are using a directory other than Oracle Internet Directory, specify the Oracle Virtual Directory host (which should be IDSTORE.*mycompany*.com.)
   - IDSTORE_BINDDN Is an administrative user in the identity store directory.

- IDSTORE_USERSEARCHBASE is the location in the directory where users are stored.
- IDSTORE_GROUPSEARCHBASE is the location in the directory where groups are stored.
- IDSTORE_SEARCHBASE is the location in the directory where users and groups are stored.
- IDSTORE_SYSTEMIDBASE is the location of a container in the directory where users can be placed when you do not want them in the main user container. This happens rarely but one example is the Oracle Identity Manager reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.

Name this file `preconfigPropertyFile` or similar as you will use it to preconfigure the identity store in the next step.

5. Use this properties file to perform general configuration of the identity store with the following command:

```
idmConfigTool -preConfigIDStore input_file=propertiesFile
```

6. Create a second properties file with contents as shown here:

```
IDSTORE_HOST : idstore.mycompany.com
IDSTORE_PORT : 389
IDSTORE_BINDDN : cn=orcladmin
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=mycompany,dc=com
IDSTORE_READONLYUSER: IDROUser
IDSTORE_READWRITEUSER: IDRWUser
IDSTORE_SUPERUSER: weblogic_admin
IDSTORE_OAMSOFTWAREUSER: oamLDAP
IDSTORE_OAMADMINUSER: oamadmin
IDSTORE_OIMADMINUSER: oimadmin
IDSTORE_OIMADMINGROUP: OIMAdmins
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdmins
```

where:

- `IDSTORE_HOST` and `IDSTORE_PORT` are the host and port, respectively, of your identity store directory. If you are using a directory other than Oracle Internet Directory, specify the Oracle Virtual Directory host (which should be IDSTORE.*mycompany*.com.)
- `IDSTORE_BINDDN` is an administrative user in the identity store directory.
- `IDSTORE_USERSEARCHBASE` is the location in the directory where users are stored.
- `IDSTORE_GROUPSEARCHBASE` is the location in the directory where groups are stored.
- `IDSTORE_SEARCHBASE` is the location in the directory where users and groups are stored.
- `IDSTORE_SYSTEMIDBASE` is the location of a container in the directory where users can be placed when you do not want them in the main user container.

This happens rarely but one example is the Oracle Identity Manager reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.

- `IDSTORE_SYSTEMIDBASE` is the location in your directory where the Oracle Identity Manager reconciliation user are placed.
- `IDSTORE_READONLYUSER` is the name of a user you want to create which has Read Only permissions on your Identity Store.
- `IDSTORE_READWRITEUSER` is the name of a user you want to create which has Read/Write permissions on your identity store.
- `IDSTORE_SUPERUSER` is the name of the administration user you want to use to log in to the WebLogic Administration Console in the Oracle Fusion Applications domain.
- `IDSTORE_OAMSOFTWAREUSER` is a user that gets created in LDAP that is used when Oracle Access Manager is running to connect to the LDAP server.
- `IDSTORE_OAMADMINUSER` is the name of the user you want to create as your Oracle Access Manager Administrator.
- `IDSTORE_OIMADMINUSER` is the name of the administration user you would like to use to log in to the Oracle Identity Manager console.
- `IDSTORE_OIMADMINGROUP` is the name of the group you want to create to hold your Oracle Identity Manager administrative users.
- `OAM11G_IDSTORE_ROLE_SECURITY_ADMIN` is the name of the group to hold users who have access to the Oracle Access Manager administration console.

Name this file preparePropertyFile or similar as you will use it to prepare the identity store in the next step.

7. Use this properties file to perform component-specific configuration of the identity store for integration using the following command:

```
idmConfigTool -prepareIDStore mode=all input_file=propertiesFile
```

8. Perform the following tasks for Oracle Identity Manager:

   a. Configure LDAP synchronization (LDAP sync) in the domain where Oracle Identity Manager runs. Confirm that LDAP sync is operational before continuing.

   Note: When loading schemas as part of this step, first load the Oracle Access Manager schema and then load the Oracle Identity Manager schema.

   For information about configuring LDAP synchronization, see the following sections in Chapter 15, "Configuring Oracle Identity Manager" of the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*: "Completing the Prerequitistes for Enabling LDAP Synchronization", "Running the LDAP Post-Configuration Utility", and "Verifying the LDAP Synchronization".

   b. Using Oracle Directory Services Manager, configure the Oracle Virtual Directory adapters created in Step 8a to set the `oamEnabled` parameter to `true`.

c. In the domain running Oracle Identity Manager, execute the Oracle Identity Manager configuration wizard with the LDAP sync option enabled.

Notes:

- These instructions assume that your directory server is Oracle Internet Directory. If using a different directory server, additional configuration may be required; see the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management* for details.
- Before proceeding to the next step, ensure that an Oracle Identity Manager administrator account exists in the directory and is enabled.

9. Verify that the WebLogic managed servers for Oracle Access Manager and Oracle Identity Manager are shut down.
10. Restart the Oracle WebLogic Server Administration Server.

    See Also: See *Stopping or Starting the Oracle Stack* in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

11. Configure logout for the IDM domain agent. For details, see Configuring Centralized Logout for the IDM Domain Agent in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

5.3 Perform Integration Tasks in Oracle Access Manager

Take these steps to integrate Oracle Access Manager with Oracle Identity Manager and the directory server:

1. Set the environment variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME` and `ORACLE_HOME`.

   Set `IDM_HOME` to `IDM_ORACLE_HOME`, where Oracle Internet Directory is installed.

   Set `ORACLE_HOME` to `IAM_ORACLE_HOME`, where Oracle Access Manager and Oracle Identity Manager are installed.

2. Update the domain agent password as follows:

   a. Log in to the Oracle Access Manager console:

      `http:`*`oam_admiserver_host:port`*`/oamconsole`

   b. Navigate to the **system configuration** tab, then **Access Manager Settings**, then **SSO Agents**.

      Double-click "OAM Agents", which opens a Webgate page on the right.

      Click **Search** to list all webgate agents including "`IAMSuiteAgent`".

      Double-click it to edit the `IAMSuiteAgent` agent. Update the field "`Access Client Password`" with the desired password.

   c. Log in to the Oracle WebLogic Server console:

      `http:`*`oam_adminserver_host:port`*`/console`

d. Navigate to **Security Realms**, then **myrealm**. Open the **providers** tab and edit `IAMSuiteAgent`.

Open the **Provider Specific** tab and update the agent password. Save the changes.

e. Restart the Oracle Access Manager managed server.

You will use the updated password in Step 4 below.

3. Create a properties file with the following contents:

```
WLSHOST: adminvhn.mycompany.com
WLSPORT: 7001
WLSADMIN: weblogic
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_USERSEARCHBASE: cn=Users,mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_OAMSOFTWAREUSER: oamLDAP
IDSTORE_OAMADMINUSER: oamadmin
PRIMARY_OAM_SERVERS: oamhost1.mycompany.com:5575,oamhost2.mycompany.com:5575
WEBGATE_TYPE: ohsWebgate10g
ACCESS_GATE_ID: IAMSuiteAgent
COOKIE_DOMAIN: .us.example.com
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
OAM_TRANSFER_MODE: OPEN
OAM11G_SSO_ONLY_FLAG: true
OAM11G_OIM_INTEGRATION_REQ: true
OAM11G_OIM_OHS_URL:https://sso.mycompany.com:443/
COOKIE_EXPIRY_INTERVAL: 120
```

Where:

- `WLSHOST` and `WLSPORT` are, respectively, the host and port of your administration server, this will be the virtual name.
- `WLSADMIN` is the WebLogic administrative user you use to log in to the WebLogic console.
- `IDSTORE_HOST` and `IDSTORE _PORT` are, respectively, the host and port of your Identity Store directory.

Note: If using a directory server other than Oracle Internet Directory, specify the Oracle Virtual Directory host and port.

- `IDSTORE_BINDDN` is an administrative user in Oracle Internet Directory.

Note: If using a directory server other than Oracle Internet Directory, specify an Oracle Virtual Directory administrative user.

- `IDSTORE_USERSEARCHBASE` is the location in the directory where users are stored.

- IDSTORE_GROUPSEARCHBASE is the location in the directory where groups are stored.
- IDSTORE_SEARCHBASE is the location in the directory where users and groups are stored.
- IDSTORE_OAMSOFTWAREUSER is the name of the user you use to interact with LDAP.
- IDSTORE_OAMADMINUSER is the name of the user you use to access your Oracle Access Manager console.
- PRIMARY_OAM_SERVERS is a comma-separated list of your Oracle Access Manager servers and the proxy ports they use.

Note: To determine the proxy ports your Oracle Access Manager servers use:

1. Log into the Oracle Access Manager console at `http://admin.mycompany.com:7001/oamconsole`
2. Click the **System Configuration** tab.
3. Expand **Server Instances** under the Common Configuration section
4. Click on an Oracle Access Manager server, such as **WLS_OAM1**, and click **Open**.
5. Proxy port is shown as **Port**.

- WEBGATE_TYPE is the type of WebGate agent you want to create.
- ACCESS_GATE_ID is the name you want to assign to the WebGate. Do *not* change the property value shown above.
- COOKIE_DOMAIN is the domain in which the WebGate functions.
- OAM_TRANSFER_MODE is the security model in which the access servers function.
- OAM11G_SSO_ONLY_FLAG determines whether Oracle Access Manager is used in authentication-only mode.
- OAM11G_OIM_OHS_URL is the URL of the load balancer fronting the Oracle HTTP servers.

Name this file OAMconfigPropertyFile or similar as you will use it to configure Oracle Access Manager in the next step.

4. Configure Oracle Access Manager using the command idmConfigTool, which is located at:

```
IAM_ORACLE_HOME/idmtools/bin
```

The command syntax is as follows:

```
idmConfigTool -configOAM input_file=propertiesFile
```

5.4 Perform Integration Tasks in Oracle Identity Manager

Integrate Oracle Identity Manager with Oracle Access Manager by performing the following steps:

1. On the machine where Oracle WebLogic Server and Oracle Identity Manager Server are installed, create the `wlfullclient.jar` file as follows:
   1. Navigate to the `MW_HOME/wlserver_10.3/server/lib` directory.
   2. Set your `JAVA_HOME` to `MW_HOME/jdk160_18` and ensure that your `JAVA_HOME/bin` directory is in your path.
   3. Create the `wlfullclient.jar` file by running:

      ```
      java -jar wljarbuilder.jar
      ```

   Verify that the jar file was created.
2. Set the environment variables: `MW_HOME`, `JAVA_HOME`, `IDM_HOME` and `ORACLE_HOME`.

   Set `IDM_HOME` to `IDM_ORACLE_HOME`, where Oracle Internet Directory is installed.

   Set `ORACLE_HOME` to `IAM_ORACLE_HOME`, where Oracle Access Manager and Oracle Identity Manager are installed.
3. Create a properties file with contents as in the following:

```
LOGINURI: /${app.context}/adfAuthentication
LOGOUTURI: /oamsso/logout.html
AUTOLOGINURI: /obrar.cgi
ACCESS_SERVER_HOST: OAMHOST1.mycompany.com
ACCESS_SERVER_PORT: 5575
ACCESS_GATE_ID: IAMSuiteAgent
COOKIE_DOMAIN: .mycompany.com
COOKIE_EXPIRY_INTERVAL: 120
OAM_TRANSFER_MODE: SIMPLE
WEBGATE_TYPE: javaWebgate
SSO_ENABLED_FLAG: true
IDSTORE_PORT: 389
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_DIRECTORYTYPE: OID
IDSTORE_ADMIN_USER: oamdmin. Note that the entry contain the complete LDAP DN
of the user (the username alone in insufficient).
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
MDS_DB_URL: jdbc:oracle:thin:@DBHOST:PORT:SID
MDS_DB_SCHEMA_USERNAME: edg_mds
WLSHOST: adminvhn.mycompany.com
WLSPORT: 7001
WLSADMIN: weblogic
DOMAIN_NAME: IDM_Domain
OIM_MANAGED_SERVER_NAME: WLS_OIM1
DOMAIN_LOCATION: ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain
```

Notes:

- The ACCESS_SERVER_PORT must be the Oracle Access Manager NAP port.
- If your access manager servers are configured to accept requests using the simple mode, set `OAM_TRANSFER_MODE` to `SIMPLE`. Otherwise set `OAM_TRANSFER_MODE` to `OPEN`.
- Set `WEBGATE_TYPE` to `javaWebgate` if using a domain agent; set it to `ohsWebgate10g` if using a 10*g* WebGate.
- Set `IDSTORE_PORT` to your Oracle Internet Directory port.
- Set `IDSTORE_HOST` to your Oracle Internet Directory host or load balancer name.
- MDS_DB_URL in this case represents a single instance database. The string following the '`@`' symbol must have the correct values for your environment. SID must be the actual SID, *not* a service name.
- The value of `IDSTORE_ADMIN_USER` must contain the complete LDAP DN of the user. The entry should be similar to "cn=oamadmin,cn=Users,dc=us,dc=oracle,dc=com" instead of just "oamadmin".

Name this file `OIMconfigPropertyFile` or similar as you will use it to configure Oracle Identity Manager in Step 4.

4. Change location to: *`IAM_ORACLE_HOME`*`/server`

   ```
   cd IAM_ORACLE_HOME/server
   ```

5. Integrate Oracle Access Manager with Oracle Identity Manager using the command `idmConfigTool`, which is located at:

   `IAM_ORACLE_HOME``/idmtools/bin`

   The syntax of the command is

   ```
   idmConfigTool -configOIM input_file=propertiesFile
   ```

   where `propertiesFile` is the file you set up in Step 2.

   When the command executes you will be prompted for:

   - Access Gate Password
   - Single Sign-On (SSO) Keystore Password
   - Global Passphrase
   - Idstore Admin Password
   - MDS Database schema password
   - Admin Server User Password
   - Password to be used for Oracle Access Manager administrative user

6. Check the log file for errors and correct them if necessary.
7. Restart the Oracle Identity Manager managed server and the WebLogic Administration Server.

5.5 Test the Integration

The final task is to verify the integration by performing, in order, the steps shown in Table 5–1:

Table 5–1 Verifying Oracle Access Manager-Oracle Identity Manager Integration

Step	Description	Expected Result
1	Access the Oracle Access Manager Administration Console using the URL: `http://admin_server_host:admin_server_port/oamconsole`	Provides access to the console. The credential collector URL should be the Oracle Access Manager Managed Server URL.
2	Access the Oracle Identity Manager administration page with the URL: `http://oimhost:oimport/admin/faces/pages/Admin.jspx`	The Oracle Access Manager login page from the Oracle Access Manager managed server should appear. Check that the links for "Forgot Password", "Self Register" and "Track Registration" appear on the login page.
3	Log in as an Oracle Identity Manager administrator (the user referred to in Step 6 of Section 5.2).	The Oracle Identity Manager Admin Page should be accessible.
4	Create a new user on the Oracle Identity Manager Admin Page. Close the browser and try accessing the Oracle Identity Manager Admin Pages. When prompted for login, provide valid credentials for the newly-created user.	You should be redirected to Oracle Identity Manager and required to reset the password.
5	Close the browser and access the Oracle Identity Manager Admin Page.	The Oracle Access Manager login page from the Oracle Access Manager managed server should come up. Verify that the links for "Forgot Password", "Self Register" and "Track Registration" are available in the login page. Check that each link works.
6	To check that lock/disable works, open a browser and log in as a test user. In another browser session, log in as xelsysadm and lock the test user account. Click the **Logout** link on the OIM console.	The user must be logged out and redirected back to the login page.
	To test SSO logout, log in to the Oracle Identity Manager console as test user/xelsysadm.	Upon logout from the page, it must redirect to the SSO logout page.

5.6 Additional Configuration

This section describes additional configuration that you may need to perform depending on your requirements.

5.6.1 Migrating from the Domain Agent to 10gWebGate with OHS 11g

Perform this task by following the instructions in *Migrating from Domain Agent to Oracle HTTP Server 10g Webgate for OAM* in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Next, complete the configuration by performing these actions:

- Update WebGate Type and ID

- Set the WebGate Preferred Host
- Create the Oracle Identity Manager SSO Keystore

5.6.1.1 Update WebGate Type and ID

Take these steps to update the Webgate Type and WebGate ID using Oracle Enterprise Manager Fusion Middleware Control:

1. Navigate to **Identity and Access**, then **OIM**, then **oim(11.1.1.3.0)**.
2. Right-click on **oim (11.1.1.3.0)** and select **System Mbean Browser**.
3. Navigate to **Application Defined Mbeans**, then **oracle.iam**, then Server: oim_server1, then Application:oim, then **XMLConfig**, then **Config**, then **XMLConfig.SSOConfig**, then **SSOConfig**.

5.6.1.2 Set the WebGate Preferred Host

This step is required to redirect users to the Oracle Access Manager login page for Oracle Identity Manager if they type in a URL of the form:

`http://OHS_HOST:OHS_PORT/admin/faces/pages/Admin.jspx`

Take these steps to set the preferred Webgate host:

1. Log in to the Oracle Access Manager console, Click on **System Configuration**, and navigate to **Access Manager Settings**, then **SSO Agents**, then **OAM Agent**.
2. Click the **Search** button. A list of WebGate IDs appears. Open the one registered in WebGate.
3. Update the Preferred Host field and set it to IAMSuiteAgent.
4. Click **Apply**.
5. Restart Oracle HTTP Server.

5.6.1.3 Create the Oracle Identity Manager SSO Keystore

> **Note:** This step is needed if WebGate is configured in simple mode.

Follow the instructions in *Creating Oracle Identity Manager SSO Keystore* in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

5.6.2 Loading the Nexaweb Applet in an Integrated Environment

In an Oracle Identity Manager and Oracle Access Manager (OAM) integrated environment, when you login to the Oracle Identity Manager Administrative and User Console and click a link that opens the Nexaweb applet, configuration is required to enable loading of the NexaWeb Applet. The steps are as follows:

1. Log in to the Oracle Access Manager Console.
2. Create a new Webgate ID. To do so:
   a. Click the **System Configuration** tab.
   b. Click **10Webgates**, and then click the Create icon.
   c. Specify values for the following attributes:

      Name: *NAME_OF_NEW_WEBGATE_ID*

Access Client Password: *PASSWORD_FOR_ACCESSING_CLIENT*

Host Identifier: IAMSuiteAgent

d. Click **Apply**.

e. Edit the Webgate ID, as shown:

set 'Logout URL' = /oamsso/logout.html

f. Deselect the **Deny On Not Protected** checkbox.

3. Install a second Oracle HTTP Server (OHS) and Webgate. During Webgate configurations, when prompted for Webgate ID and password, use the Webgate ID name and password for the second Webgate that you provided in step 2c.
4. Login to the Oracle Access Manager Console. In the Policy Configuration tab, expand Application Domains, and open IdMDomainAgent.
5. Expand Authentication Policies, and open Public Policy. Remove the following URLs in the Resources tab:

   /xlWebApp/.../*

   /xlWebApp

   /Nexaweb/.../*

   /Nexaweb

6. Expand Authorization Policies, and open Protected Resource Policy. Remove the following URLs in the Resources tab:

   /xlWebApp/.../*

   /xlWebApp

   /Nexaweb/.../*

   /Nexaweb

7. Restart all the servers.
8. Update the obAccessClient.xml file in the second Webgate. To do so:

   a. Create a backup of the *SECOND_WEBGATE_HOME*/access/oblix/lib/ObAccessClient.xml file.

   b. Open the *DOMAIN_HOME*/output/*WEBGATE_ID_FOR_SECOND_WEBGATE*/ObAccessClient.xml file.

   Note: Ensure that the DenyOnNotProtected parameter is set to 0.

   c. Copy the *DOMAIN_HOME*/output/*WEBGATE_ID_FOR_SECOND_WEBGATE*/ObAccessClient.xml file to the *SECOND_WEBGATE_HOME*/access/oblix/lib/ directory.

9. Copy the mod_wls_ohs.conf from the *FIRST_OHS_INSTANCE_HOME*/config/*OHS_NAME*/directory to the *SECOND_OHS_INSTANCE_HOME*/config/*OHS_NAME*/ directory. Then, open the mod_wls_host.conf of the second OHS to ensure the WebLogicHost and WeblogicPort are still pointing to Oracle Identity Manager managed server host and port.
10. Remove or comment out the following lines in the *SECOND_OHS_INSTANCE_HOME*/config/*OHS_NAME*/httpd.conf file:

```
<LocationMatch "/oamsso/*">
   Satisfy any
</LocationMatch>
```

11. Copy the logout.html file from the FIRST_WEBGATE_HOME/access/oamsso/ directory to the SECOND_WEBGATE_HOME/access/oamsso/ directory. Then, open the logout.html file of the second Webgate to ensure that the host and port setting of the SERVER_LOGOUTURL variable are pointing to the correct OAM host and port.
12. Login to Oracle Access Manager Console. In the Policy Configuration tab, expand **Host Identifiers**, and open the host identifier that has the same name as the second Webgate ID name. In the Operations section, verify that the host and port for the second OHS are listed. If not, then click the add icon (+ sign) to add them. Then, click **Apply**.
13. Use the second OHS host and port in the URL for the OAM login page for Oracle Identity Manager. The URL must be in the following format:

    http://*SECOND_OHS_HOST*:*SECOND_OHS_PORT*/admin/faces/pages/Admin.jspx

6

Integrating Oracle Access Manager and Oracle Adaptive Access Manager

This chapter explains how to integrate Oracle Adaptive Access Manager with Oracle Access Manager to provide advanced login security. The integration includes virtual authentication devices, device fingerprinting, real-time risk analysis, and risk-based challenge authentication.

This chapter contains these sections:

Note: Integration with Oracle Identity Manager provides additional features related to password collection. See Chapter 7, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager".

See Also: Chapter 2, "Introduction to Oracle Access Manager Integrations".

6.1 About Basic and Advanced Integration Modes

There are several types of Oracle Access Manager and Oracle Adaptive Access Manager integration. *Basic* requires less server resources and offers a subset of functionality where *Advanced* requires an additional managed server but is not limited in functionality.

Table 6–1 summarizes the Oracle Access Manager and Oracle Adaptive Access Manager integrations types.

Table 6–1 Types of Oracle Access Manager-Oracle Adaptive Access Manager Integration

Details	Basic	Advanced	Advanced Using TAP
Available	11.1.1.3.0	11.1.1.3.0	11.1.1.5.0
Description	The Basic integration embeds the Oracle Adaptive Access Manager server into Oracle Access Manager. It includes the libraries and configuration interface for different flows (challenge, registration, and so on) and reduces the footprint. **Note:** The OAAM Server is embedded in the Oracle Access Manager Server, but you will still need a separate managed server for the OAAM Admin application.	The Advanced integration option includes OTP Anywhere, a challenge processor framework, the shared library framework, and the secure self-service password management flows.	The Advanced integration option using TAP includes all the features of the 11g (11.1.1.3) integration and supports the use of both 10g and 11*g* agents.
Supported Agents	10*g* WebGate and OSSO Agent	10*g* WebGate	10*g* and 11*g* WebGates
Authentication Scheme	The native integration offers the OAAMBasic authentication scheme out-of-the-box. For information about the scheme, see "Managing Authentication Schemes" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.	OAAMAdvanced authentication scheme	tapScheme
Where information is located	Section 6.2, "Oracle Access Manager-Oracle Adaptive Access Manager Basic Integration"	Section 6.3, "Oracle Access Manager-Oracle Adaptive Access Manager Advanced Integration"	Chapter 7, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager"

6.2 Oracle Access Manager-Oracle Adaptive Access Manager Basic Integration

Oracle Access Manager and Oracle Adaptive Access Manager Basic integration, which is a native integration, requires the OAM server and OAAM Admin Server in the IDM Middleware WebLogic Domain and a functional OAAM database. The OAAM Admin Server is used by Oracle Access Manager Administrators to import and export policies, create new policies, view sessions, and configure Oracle Adaptive Access Manager functionality. When policies are imported, exported, or configured, the changes are saved to the OAAM database.

The Oracle Adaptive Access Manager libraries are bundled with the Oracle Access Manager server. Oracle Access Manager is integrated with Oracle Adaptive Access Manager through the extension libraries and uses them directly. The rules engine and the runtime functionality of Oracle Adaptive Access Manager are provided using these libraries. When a user enters the registration flow, Oracle Access Manager shows the user the virtual authentication devices and runs the pre-authentication policies by using the OAAM libraries to make API calls. The OAAM libraries internally make JDBC calls to save the data related to the user to the OAAM database. The OAAM Server is not needed in this deployment since the Oracle Adaptive Access Manager

runtime functionalities are available through the libraries. Knowledge-based Authentication (KBA) is the only challenge mechanism available in this integration.

This section explains how to integrate Oracle Access Manager (OAM) 11g and Oracle Adaptive Access Manager (OAAM) 11g as a Basic integration.

> **See Also:** Section 2.8.2, "Deployment Options for Strong Authentication".

The following topics explain how this type of integration is implemented:

- Processing Flow for Native Integration
- Prerequisites
- Native Integration Steps

6.2.1 Processing Flow for Native Integration

The flow is as follows:

1. The Oracle Access Manager server receives a request for a page protected by an Oracle Access Manager WebGate.
2. Oracle Access Manager calls the Oracle Adaptive Access Manager APIs to execute the pre-authentication rules. Based on the result (allow/block/deny), Oracle Access Manager displays the appropriate pages to collect credentials. Oracle Access Manager performs all the processing, never passing control to Oracle Adaptive Access Manager.
3. Oracle Access Manager collects the user credentials.
4. Oracle Access Manager verifies the credentials against the identity store.
5. To run post-authentication rules, Oracle Access Manager calls the Oracle Adaptive Access Manager APIs again. Based on the result (register user, register questions, register user [optional], challenge, allow, or block), Oracle Access Manager renders the appropriate set of pages.

   For example, if the result of the rule check is a challenge, Oracle Access Manager renders a challenge question page with the security question displayed.

6.2.2 Prerequisites

Take the following steps to prepare for the integration procedure:

1. Install the Oracle Database.
2. Create and load the Oracle Access Manager and Oracle Adaptive Access Manager schemas in the database.

   See the *Oracle Fusion Middleware Repository Creation Utility User's Guide* for instructions on running the Repository Creation Utility to create the Oracle Access Manager and Oracle Adaptive Access Manager schemas in the database repository.
3. Install WebLogic Servers

   See the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* for complete information on installing the Oracle WebLogic Server.
4. Install Oracle Access Manager and Oracle Adaptive Access Manager.

See the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* for instructions on installing Oracle Access Manager and Oracle Adaptive Access Manager.

5. Patch the software to the latest version.
6. Run the Oracle Identity Management 11*g* Configuration Wizard to configure Oracle Adaptive Access Manager in a new WebLogic administration domain or in an existing one.

   Refer to "*Configuring Oracle Adaptive Access Manager*" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* for instructions on configuring Oracle Adaptive Access Manager.
7. Start the Administration Server for the WebLogic domain.

   For UNIX systems:

   ```
   DOMAIN_HOME/bin/startWebLogic.sh
   ```

   For Windows systems:

   ```
   DOMAIN_HOME\bin\startWebLogic.cmd
   ```

6.2.3 Native Integration Steps

Follow the steps in this section to implement the Oracle Access Manager and Oracle Adaptive Access Manager integration.

If you prefer to use the `configureOAAM` WLST command to create the data source, associate it as a target with the OAM server, and enable the property in the `oam-config.xml`, refer to "Using ConfigureOAAM WLST to Create the Datasource".

1. Locate and modify the `oam-config.xml` file manually.

   The `oam-config.xml` file contains all OAM-related system configuration data and is located in the *DOMAIN_HOME*`/config/fmwconfig` directory.

   Set the `OAAMEnabled` property to `true` as shown in the following example:

   ```
   <Setting Name="OAAM" Type="htf:map">
   <Setting Name="OAAMEnabled" Type="xsd:boolean">true</Setting>
   <Setting Name="passwordPage"
   Type="xsd:string">/pages/oaam/password.jsp</Setting>
   <Setting Name="challengePage"
   Type="xsd:string">/pages/oaam/challenge.jsp</Setting>
   <Setting Name="registerImagePhrasePage"
   Type="xsd:string">/pages/oaam/registerImagePhrase.jsp</Setting>
   <Setting Name="registerQuestionsPage"
   Type="xsd:string">/pages/oaam/registerQuestions.jsp</Setting>
   ```

2. Navigate to the Oracle Access Manager Administration Console:

   ```
   http://oam_admin_server_host:oam_admin_server_port/oamconsole
   ```

3. Select **Resources** under **IDMDomainAgent**.
4. Add the protected resource.

   For example, provide the following information for the resource:

   - **Host Identifier**: `IDMDomain`
   - **Resource URL**: `/<resource>/.../*`

5. Create a new Authentication Policy under **IDMDomainAgent** and make sure to set the Authentication Scheme to `OAAMBasic`.

   In this step, you are associating the protected resource with the `OAAMBasic` Authentication Scheme.

6. Create a user that has the correct privileges to log in to the Oracle Adaptive Access Manager Administration Console and then grant the necessary groups to the user.

   For information, refer to "Creating OAAM Users" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

7. Start the OAAM Admin Server, `oaam_admin_server1`, to register the newly created managed servers with the domain.

   For UNIX systems, start the OAAM Administration Server by using the `startManagedWebLogic.sh` command, which is located in the *DOMAIN_HOME*`/bin` directory:

   ```
   startManagedWebLogic.sh oaam_admin_server1
   ```

   For Windows systems, start the OAAM Administration Server by using the `startManagedWebLogic.cmd` command, which is located in the *DOMAIN_HOME*`\bin` directory:

   ```
   startManagedWeblogic.cmd oaam_admin_server1
   ```

8. Log in to the OAAM Administration Console as an Oracle Adaptive Access Manager Administrator:

   `http://`*`oaam_managed_server_host`*`:14200/oaam_admin`

9. Import the Oracle Adaptive Access Manager snapshot into the system using the Oracle Adaptive Access Manager Administration Console. The snapshot contains policies, challenge questions, dependent components, and configurations that are required by Oracle Adaptive Access Manager.

   For instructions on importing the snapshot, refer to "Importing the OAAM Snapshot" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

10. Shut down the OAAM Administration Server, `oaam_admin_server1`.

    For UNIX systems, stop the OAAM Administration Server by using the `stopManagedWebLogic.sh` command, which is located in the *DOMAIN_HOME*`/bin` directory:

    ```
    stopManagedWebLogic.sh oaam_admin_server1
    ```

    For Windows systems, stop the OAAM Administration Server by using the `stopManagedWebLogic.cmd` command, which is located in the *DOMAIN_HOME*`\bin` directory:

    ```
    stopManagedWeblogic.cmd oaam_admin_server1
    ```

11. Access the Oracle WebLogic Administration Console:

    `http://`*`weblogic_admin_server`*`:7001/console`

12. If Oracle Adaptive Access Manager is not configured to be in the same WebLogic domain as Oracle Access Manager, perform the following steps for Oracle Access Manager:

    - Create a datasource with the following JNDI name:

```
jdbc/OAAM_SERVER_DB_DS
```

Note: The name of the datasource can be any valid string, but the JNDI name should be as shown above.

- To the schema you created as part of the Oracle Adaptive Access Manager configuration, provide the connection details for the Oracle Adaptive Access Manager database.

13. Click **Services** and then **Database Resources** and locate the **OAAM_SERVER_DB_DS** resource.
14. Lock the environment by clicking the **Lock** button in the upper left corner of the WebLogic Administration Console.
15. Open the **OAAM_SERVER_DB_DS** resource and click the **Target** tab. Once there, you are presented a list of WebLogic servers that are available.
16. Associate **Administration Server** and **oam_server1** as targets with the datasource.
17. Click the **Activate** button in the upper left corner of the Oracle WebLogic Administration Console.
18. Start the OAM Server, `oam_server1`.

    For UNIX systems, start the OAM Server by using `startManagedWebLogic.sh`, which is located in *DOMAIN_HOME*`/bin`:

    ```
    startManagedWebLogic.sh oam_server1
    ```

    For Windows systems, start the OAM Server by using `startManagedWebLogic.cmd`, which is located in *DOMAIN_HOME*`\bin`:

    ```
    startManagedWeblogic.cmd oaam_server1
    ```

19. Access the protected resource to verify the configuration.

    At this point the configuration of Oracle Adaptive Access Manager is completed. To test the configuration go to:

    ```
    http://admin_server:7001/resource
    ```

    You are prompted to enter a user name. Then, on a separate screen you are prompted for the password.

    Once the user name and password are validated you are asked to answer challenge questions. Once completed you are taken to the protected application.
20. For further testing, remote-register two agents, each protecting a resource.
21. Use the Administration Console to associate the first resource with the `OAAMBasic` policy for the authentication flow. Associate the second resource with the `LDAPScheme`.

See Also: "Managing Authentication Schemes" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

6.3 Oracle Access Manager-Oracle Adaptive Access Manager Advanced Integration

Integrating Oracle Adaptive Access Manager with Oracle Access Manager provides an enterprise with advanced access security features that greatly improve the level of protection for applications. Features including anti-phishing, anti-malware, device fingerprinting, behavioral profiling, geolocation mapping, real-time risk analysis and multiple risk-based challenge mechanisms such as one-time password and knowledge based authentication questions provide an increased level of access security.

Features supporting the strong authentication flow for Oracle Access Manager logins are summarized in Table 6–2.

See Also: Section 2.8.2, "Deployment Options for Strong Authentication".

Table 6–2 Oracle Adaptive Access Manager Features Supporting Strong Authentication for OAM Logins

Feature	Description
Virtual authenticators	Oracle Adaptive Access Manager includes unique functionality to protect users while interacting with a protected web application. The virtual authentication devices harden the process of entering and transmitting authentication credentials and provide users with verification they are authenticating on a valid application. For details on virtual authenticators, refer to "Using Virtual Authentication Devices" in the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.
Fraud rules	Rules are used to evaluate the level of risk at each checkpoint. For information on policies and rules, refer to "OAAM Security and Autolearning Policies" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
Knowledge Based Authentication (KBA)	Knowledge-based authentication (KBA) is a secondary authentication method that provides an infrastructure for users to select questions and provide answers which are used to challenge them later on, registration logic to manage the registration of challenge questions and answers, Answer Logic to intelligently detect the correct answers in the challenge response process, and validations for answers given by a user at the time of registration. For information, refer to "Managing Knowledge-Based Authentication" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
OTP Anywhere	OTP Anywhere is a risk-based challenge solution consisting of a server generated one-time password delivered to an end user via a configured out-of-band channel. For information, refer to "Setting Up OTP Anywhere" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

6.3.1 Processing Flow for Advanced Integration

The flow of interactions between Oracle Access Manager and Oracle Adaptive Access Manager is as follows:

1. A user tries to access a resource protected by Oracle Access Manager.
2. The Oracle Access Manager WebGate intercepts the (unauthenticated) request and redirects the user to the Oracle Adaptive Access Manager Server.
3. The Oracle Adaptive Access Manager Server presents the user with the Oracle Adaptive Access Manager user name page.
4. The user submits his user name on the Oracle Adaptive Access Manager user name page.

5. Oracle Adaptive Access Manager fingerprints the user device and runs pre-authentication rules to determine if the user should be allowed to proceed to the Oracle Adaptive Access Manager password page.
6. Device fingerprinting is performed.

   Device fingerprinting is performed. Device fingerprinting is a mechanism to recognize the devices a user logs in with, whether it is a desktop computer, laptop computer, PDA, cell phone, kiosk, or other Web-enabled device.
7. If the user is allowed to proceed, the virtual authentication device rules are run during the Authentication Pad checkpoint. These rules determine which virtual authenticator to display in the Oracle Adaptive Access Manager password page.
8. If the user has registered with Oracle Adaptive Access Manager, the Oracle Adaptive Access Manager Server displays the Oracle Adaptive Access Manager password page with either the personalized TextPad or KeyPad.
9. If the user has not registered, Oracle Adaptive Access Manager displays the Oracle Adaptive Access Manager password page with the Generic TextPad.
10. The user submits his password on the Oracle Adaptive Access Manager password page.
11. The credentials collected from Oracle Adaptive Access Manager is verified against the identity store using the Oracle Access Manager NAP (Network Assertion Protocol) API. After validation on the Oracle Access Manager side, Oracle Adaptive Access Manager runs the post-authentication rules.
12. Oracle Adaptive Access Manager interacts with the user to establish identity to perform the desired action. Oracle Adaptive Access Manager determines the user's risk score and executes any actions (for example, KBA or OTP) or alerts that are specified in the policy.
13. If the user is not registered, he may be asked to go through registration, for example, KBA or OTP.
14. Registration is required depending on security requirements, which specify whether the registration is mandatory or optional.
15. If authentication is successful and the user has the appropriate profile registered, Oracle Adaptive Access Manager sets the Oracle Access Manager cookie and redirects the user to the redirect URL.

6.3.2 Implementing Advanced Integration

Advanced integration between Oracle Access Manager and Oracle Adaptive Access Manager can involve scenarios with or without Oracle Identity Manager.

With Oracle Identity Manager

Integration with Oracle Identity Manager provides users with richer password management functionality, including secure "Forgot Password" and "Change Password" flows.

For integration details, see Chapter 7, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager".

Without Oracle Identity Manager

If Oracle Identity Manager is not part of your environment, follow the integration procedure described in this chapter.

Note: To initiate logout in this scenario, access this link:

`http://host:oaam_server_port/oaam_server/oamLogout.jsp`

6.3.3 Prerequisites

To prepare for the integration procedure, ensure the necessary components have been properly installed and configured:

1. Install the Oracle Database.
2. Create and load the Oracle Access Manager and Oracle Adaptive Access Manager schemas in the database.

   See the *Oracle Fusion Middleware Repository Creation Utility User's Guide* for instructions on running the Repository Creation Utility to create the Oracle Access Manager and Oracle Adaptive Access Manager schemas in the database repository.
3. Install the Oracle WebLogic Servers

   See the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* for complete information about installing the Oracle WebLogic Server.
4. Install the Oracle SOA Suite and patch the software to the latest version.

   For information on installing the Oracle SOA Suite, refer to the *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.
5. Install and configure the Oracle Internet Directory and Oracle Virtual Directory 11*g*.

   For information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
6. Install the Oracle HTTP Server.

   For information on installing the Oracle HTTP Server, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*.
7. Install Oracle Access Manager and Oracle Adaptive Access Manager.

   At installation, Oracle Access Manager is configured with the database policy store. The Oracle Access Manager and Oracle Adaptive Access Manager wiring requires the database policy store.
8. Install the Oracle Access Manager 10*g* agent (WebGate) on the Oracle HTTP Server 11*g* instance

   For information on installing the Oracle HTTP Server WebGate, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

The following steps are based on the assumption that Oracle Access Manager and Oracle Identity Manager are integrated using the out-of-the box integration.

6.3.4 Oracle Access Manager and Oracle Adaptive Access Manager Integration Steps

> **Note:** The integration of Oracle Access Manager and Oracle Adaptive Access Manager requires that the IdentityManagerAccessGate 10gWebGate profile exist. You can validate this through the Oracle Access Manager Console by navigating to **System Configuration**, then **Agents**, then **10gWebGates**.

The high-level integration tasks consist of:

- Setting Oracle Adaptive Access Manager Properties for Oracle Access Manager
- Settingthe Oracle Access Manager Credentials in Credential Store Framework
- Configuring the Oracle Access Manager Policy Authentication Scheme

6.3.4.1 Setting Oracle Adaptive Access Manager Properties for Oracle Access Manager

> **Note:** Before performing this procedure, you must take into account whether the Oracle Adaptive Access Manager Console is being protected.
>
> - If protecting the console, you must take care of user and group creation in the external LDAP store. For details, see *Creating OAAM Administrative Groups and Users in LDAP* in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.
>
>   OR
>
> - If not protecting console, the user must be created in the Oracle WebLogic Administration Console.
>
>   (*Note*: You can disable Oracle Adaptive Access Manager administration console protection by setting the environment variable or Java property `WLSAGENT_DISABLED=`**true**.)

To set Oracle Adaptive Access Manager properties for Oracle Access Manager, follow these steps:

1. Start the managed server hosting the Oracle Adaptive Access Manager server.
2. Go to the Oracle Adaptive Access Manager Admin Console at `http://`*oaam_managed_server_host*`:`*oaam_admin_managed_server_port*`/oaam_admin`.
3. Log in as a user with access to Oracle Adaptive Access Manager environment properties.
4. Open the Oracle Adaptive Access Manager Property Editor to set the Oracle Access Manager properties.

   If a property does not exist, you must add it.

   For the following properties, set the values according to your deployment:

Table 6–3 Configuring Oracle Access Manager Property Values

Property Name	Property Values
bharosa.uio.default.password.auth.provider.classname	com.bharosa.vcrypt.services.OAMOAAMAuthProvider
bharosa.uio.default.is_oam_integrated	true
oaam.uio.oam.host	Access Server host machine name For example, *host.example.com*
oaam.uio.oam.port	Access Server Port; for example, *3004*
oaam.uio.oam.obsso_cookie_domain	Cookie domain defined in Access Server WebGate Agent
oaam.uio.oam.java_agent.enabled[1]	Default value is `false`. Set this to `true` only if the OAM Java Agent (also known as the `WLSAgent`) is used to protect the application. When setting this property, note the following points about the property `oaam.uio.oam.obsso_cookie_name`: ■ By default, the property `oaam.uio.oam.obsso_cookie_name` does not exist. ■ If using Java agent, when setting `oaam.uio.oam.java_agent.enabled` to `true`, also set the property `oaam.uio.oam.obsso_cookie_name` to the value `OAMAuthnCookie` since the Java agent uses the `OAMAuthnCookie` cookie. ■ If using WebGate Agent and `oaam.uio.oam.java_agent.enabled` is set to false, if the property `oaam.uio.oam.obsso_cookie_name` happens to be set, remove that property.
oaam.uio.oam.virtual_host_name[1]	Default value is `IDMDomain` when the OAM Java Agent (also known as the WLSAgent) is used. Change this value only if the virtual host name is different from `IDMDomain`.
oaam.uio.oam.webgate_id	IdentityManagerAccessGate The name of the WebGate Agent for Oracle Identity Manager integration. The default is IdentityManagerAccessGate.
oaam.uio.login.page	/oamLoginPage.jsp
oaam.uio.oam.secondary.host	Name of the secondary Access Server host machine. The property must be added, as it is not set by default. This property is used for high availability. You can specify the fail-over hostname using this property.
oaam.uio.oam.secondary.host.port	Port number of the secondary Access Server The property must be added as it is not set by default. This property is used for high availability. You can specify the fail-over port using this property.
oaam.oam.csf.credentials.enabled	true This property enables configuring credentials in the Credential Store Framework instead of maintaining them using the properties editor. This step is performed so that credentials can be securely stored in CSF.

[1] Required when using the OAM Java agent.

For information on setting properties in Oracle Adaptive Access Manager, see "Using the Property Editor" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

For more information about the IDM Domain Agent, see Section 1.2, "A Note About IDMDomain Agents and Webgates".

6.3.4.2 Settingthe Oracle Access Manager Credentials in Credential Store Framework

In order for Oracle Access Manager WebGate credentials to be securely stored in the Credential Store Framework, follow these steps to add a password credential to the Oracle Adaptive Access Manager domain:

1. Go to the Oracle Fusion Middleware Enterprise Manager Console:

   `http://`*`weblogic_admin_server_host:admin_server_port`*`/em`.

2. Log in as a WebLogic Administrator.
3. Expand the **Base_Domain** icon in the navigation tree in the left pane.
4. Select your domain name, right-click and select **Security**, and then select **Credentials**.
5. Click **Create Map**.
6. Click **oaam** to select the map, and then click **Create Key**.
7. In the dialog, make sure **Select Map** is **oaam**.
8. Provide the following properties and click **OK**.

Name	Value
Map Name	`oaam`
Key Name	`oam.credentials`
Key Type	*Password*
UserName	*Oracle Access Manager user with Administrator rights*
Password	*Password of Oracle Access Manager WebGate Agent*

6.3.4.3 Configuring the Oracle Access Manager Policy Authentication Scheme

Assign the Oracle Access Manager policy for the protected web application to the **OAAMAdvanced** authentication scheme using the Oracle Access Manager Administration Console.

The steps are as follows:

1. Go to the Oracle Access Manager Administration Console:

   `http://`*`hostname:port`*`/oamconsole`.

   For details, see "Logging In to the Oracle Access Manager 11*g* Administration Console" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

2. Log in as the Oracle Access Manager administrator.
3. From the **Policy Configuration** tab, navigate the tree as follows:
   - expand the Application Domains node
   - expand the IDMDomainAgent
   - expand Authentication Policies
4. Select the authentication policy named `Protected HigherLevel Policy` for editing, and assign to it the `OAAMAdvanced` authentication scheme.
5. Test the Oracle Adaptive Access Manager Challenge URL in a separate browser session by navigating to:

   `http://`*`oaam_server_managed_server:oaam_server_managed_server_port`*`/oaam_server/oamLoginPage.jsp`

6. Verify that the Oracle Adaptive Access Manager server user login page appears with no errors.

   Do *not* attempt to log in to the OAAM server yet.
7. Log in to the Oracle Access Manager Administration Console using the administrative credentials.
8. Modify the **OAAMAdvanced** authentication scheme to have the correct values for the challenge URL by making these changes:
   - Add the `challenge_url`.

     Ensure that the Oracle Adaptive Access Manager URL is correct and is the same URL that you tested in Step 5.

     `http://`*`oaam_server_managed_server_host:oaam_server_managed_server_port`*`/oaam_server/oamLoginPage.jsp`

     (*Note*: Do not use the protocol string "`http(s)`", or URL redirection will not succeed. Use an explicit protocol, either `http` or `https`.)
   - Set `contextType` to `external`.
9. Restart the Oracle Access Manager managed server.

   The steps to integrate Oracle Access Manager with Oracle Adaptive Access Manager are completed.

6.4 Configuration and Troubleshooting

This section provides troubleshooting and additional configuration topics for the integration of Oracle Access Manager and Oracle Adaptive Access Manager.

- OAAMAdvanced Authentication Scheme Protected Resource Is Not Accessible in OAM 11.1.1.4.0 - OAAM 11.1.1.5.0 Integration
- No Synchronization Between Database and LDAP

6.4.1 Using ConfigureOAAM WLST to Create the Datasource

You can use the `configureOAAM` WLST command to create the data source, associate it as a target with the OAM server, and the `OAAMEnabled` property in the `oam-config.xml` file. The syntax is as follows:

```
configureOAAM(dataSourceName,paramNameValueList)
```

where:

- `dataSourceName` is the name of the datasource to be created
- `paramNameValueList` is a comma-separated list of parameter name-value pairs. The format of each name-value pair is as follows:

  ```
  paramName='paramValue'
  ```

  The mandatory parameters are:

  - `hostName` —The name of the database host
  - `port` - the database port
  - `sid` - the database identifier (database sid)
  - `userName` - the OAAM schema name
  - `passWord` - the OAAM schema password

  The optional parameters are:

  - `maxConnectionSize` - maximum connection reserve time out size
  - `maxPoolSize` - maximum size of connection pool

For example:

```
configureOAAM(dataSourceName = "MyOAAMDS", hostName = "host.us.co.com",
port = "1521", sid = "sid", userName = "username", passWord = "password",
maxConnectionSize = None, maxPoolSize = None, serverName = "oam_server1")
```

Note: `SID` = requires the service name.

6.4.2 How to Implement Case-Insensitive Logins

After successful authentication on the Oracle Access Manager side, control is passed to Oracle Adaptive Access Manager to process the post-authentication rules. By default, if a user logging in enters the user name in mixed case using a case combination that is different from that of the registered user, the Oracle Adaptive Access Manager server will consider the user to be unregistered. For example, this happens if userxy tries to log in by entering user name userXY.

To ensure that logins are successful on both servers, you must configure the Oracle Adaptive Access Manager server to treat user names as case-insensitive. To achieve this set the following property:

```
bharosa.uio.default.username.case.sensitive=false
```

For information on setting properties in Oracle Adaptive Access Manager, see "Using the Property Editor" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

6.4.3 Using Non-ASCII Credentials

When using a non-ASCII username or password in the native authentication flow, you may encounter the following error message:

```
Sorry, the identification you entered was not recognized. Please try again.
```

Follow these steps to resolve this issue:

1. Set the PRE_CLASSPATH variable to `${ORACLE_HOME}/common/lib/nap-api.jar`.

   For C shell:

   ```
   setenv  ORACLE_HOME "IAMSUITE INSTALL DIR"
   setenv PRE_CLASSPATH "${ORACLE_HOME}/common/lib/nap-api.jar"
   ```

   For bash/ksh shell:

   ```
   export ORACLE_HOME=IAMSUITE INSTALL DIR
   export PRE_CLASSPATH="${ORACLE_HOME}/common/lib/nap-api.jar"
   ```

2. Start the managed server related to `OAAM_SERVER`.

6.4.4 Testing Before Setting Up the Integration

When setting up the environment, you may want to first test protecting a page with Oracle Access Manager only using the LDAP authentication scheme and see if you can successfully access the page. If you cannot access the page, try to resolve this issue before proceeding with the configuration.

6.4.5 OAM and OAAM Integration and Changes in the Console

In an environment where OAAMBasic integration is enabled, the following entry "`OAAMEnabled`" under oam-config.xml is set to "`true`":

```
 <Setting Name="OAAM" Type="htf:map">
      <Setting Name="OAAMEnabled" Type="xsd:boolean">true</Setting>
 </Setting>
...
```

If you see an error in OAAMBasic flows, check the value of this flag. In certain environments (Windows) or scenarios (creating a new Oracle Internet Directory and associating it with the OAAMBasic scheme) the original flows might be broken and OAAMBasic does not work because the `OAAMEnabled` flag is reset to `false`.

Workaround: Manually change the value of the flag to "true".

6.4.6 OAM and OAAM Integration and Internet Explorer Version 7

In the OAM and OAAM Basic integration mode, when you access a protected resource you are forwarded to the OAAM page. With Internet Explorer v7, after entering a username and clicking Submit, you can be stuck on the next page (/oam/pages/oaam/handleLogin.jsp) rather than being redirected to the password page automatically.

Workaround: Click the "continue" link, which brings you to /oam/pages/oaam/handleJump.jsp?clientOffset=-7.

6.4.7 OTP Challenge is Not Supported in OAAMBasic Integration

The following procedure outlines the steps required to replace the OAAM Challenge SMS policy with the OAAM Challenge policy, to prevent a challenge flow request to OTP.

During registration with Oracle Access Manager, after registering the challenge questions, you are forwarded to a contact page to enter a mobile number. In this mode of integration, with OTP unsupported, this page is not significant. You complete the registration by entering a mobile number in the following form, and Submit.

:09900502139

To modify the policies

1. Search for "OAAM Challenge Policy"
2. Under Action Group, replace "OAAM Challenge SMS" with "OAAM Challenge" every where you find it.
3. Save the policy.

6.4.8 OAAMAdvanced Authentication Scheme Protected Resource Is Not Accessible in OAM 11.1.1.4.0 - OAAM 11.1.1.5.0 Integration

An OAAMAdvanced Authentication Scheme protected resource is not accessible in an OAM 11.1.1.4.0 and OAAM 11.1.1.5.0 integration unless you perform the following:

- Set the WebGate password for OAAM.
- Set `oaam.uio.oam.authenticate.withoutsession` to `false`. By default, this is set to `true` and the `authnwithoutsession` opcode, which is not supported in OAM 11.1.1.4.0, is used.

6.4.9 No Synchronization Between Database and LDAP

Registered status records remain in the OAAM database even if registered users are removed from LDAP. When the user is added to LDAP again, the old image, phrase, and challenge questions are used, because the OAAM database and LDAP are not synched.

7

Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager

This chapter describes how to integrate Oracle Access Manager with Oracle Identity Manager and Oracle Adaptive Access Manager to provide highly secure self-service password management flows.

This chapter contains these sections:

7.1 Introduction

In the 11g Release 1 (11.1.1), Oracle Access Manager does not provide its own identity service. Instead, Oracle Access Manager provides the following:

- It consumes identity services provided by Oracle Identity Manager, LDAP directories, and other sources.
- It integrates with Oracle Identity Manager and Oracle Adaptive Access Manager to deliver a range of secure password collection and challenge-related functionality to Oracle Access Manager protected applications.

Lost password management starts off from Oracle Access Manager login page but using OAAM challenge questions and synchronized to user repositories through OIM.

Although other combinations are possible, integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager is the recommended option and provides these features:

- Password entry and malware protection through personalized virtual authentication devices
- Knowledge Based Authentication (KBA), secondary login authentication, used for all flows including risk-based authentication at login and password resets
- One-Time Password (OTP) challenge for secondary login authentication based on risk
- Registration flows to support password protection and KBA and OTP challenge functionality
- User preference flows to support password protection and KBA and OTP challenge functionality
- Password management flows

Oracle Adaptive Access Manager

Oracle Adaptive Access Manager is responsible for:

- Running real-time risk analysis rules before and after authentication
- Navigating the user through login, challenge, registration, and self-service flows

Oracle Identity Manager

Oracle Identity Manager is responsible for:

- Provisioning users (to add, modify, or delete users)
- Managing passwords (to reset or change passwords)

Oracle Access Manager

Oracle Access Manager is responsible for:

- Authenticating and authorizing users
- Providing advanced status flags such as Reset Password, Password Expired, User Locked, and others

7.2 Process Flow

In this deployment, the process flow is as follows:

Resource Protection and Credential Collection Flow

1. The OAM WebGate server is in charge of protecting the URLs and redirecting the users when they are not authenticated so they can be authenticated.
2. OAAM collects the username and password for authentication.

   So when the OAM WebGate finds that the user is not authenticated and trying to access the protected URL, it redirects the user to the OAAM Server login page.
3. The credentials are split into two different pages: a username page and a password page. OAAM allows the user to enter his username. If he is a registered

user and based on his registration status, OAAM presents the password page with his personalized image and caption.

4. The OAAM Server runs the pre-authentication rules and lets the user enter his password.
5. Since OAAM Server has the user's username and he has entered his password, the OAAM Server makes a NAP API call to the OAM Server for authentication.
6. Once the OAM server returns the status, which indicates whether the user has entered his username and password correctly, the OAAM Server determines whether the authentication was successful or not.
7. If the authentication was successful, the OAAM Server redirects the user to the OAM WebGate.
8. The OAM WebGate server redirects the user to his original URL.
9. The OAM WebGate allows the user to access the protected URL.

Reset Password Flow

1. OAAM Server communicates with the OIM server when the OAAM Server needs to call the OIM server for the password policy text that is shown when user is trying to change his password.
2. Based on the policy, OAAM Server enables the user to enter a password that meets the policy text requirements.

   Because the OAAM Server manages the flows, it is the one that presents the user with the pages where the user can enter his new password and old password.

   The text is maintained by the OAM server, but it is the OAAM server that makes the calls to get that password policy text so that it is displayed when the user tries to change his password.
3. After he finishes the task, the OAAM Server makes an API call to propagate the changes to the OAM Server.

   The OAM Server can persist those changes to the user directory or where the credentials are maintained.

   The OAM Server and OIM Server communicate with the same user directory where all the user data is maintained.

7.3 Prerequisites for the Integration

The following must be in place for the integration:

- All necessary components must be properly installed and configured:
  - Oracle Internet Directory 11*g* installed

    For information on installing Oracle Internet Directory, refer to *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
  - Oracle Virtual Directory 11*g* installed

    For information on installing Oracle Virtual Directory, refer to *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
  - Repository Creation Utility 11*g* installed

    For information on installing and using RCU, refer to *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

  - Oracle WebLogic Servers for Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Identity Manager, and Oracle HTTP Server installed

    For information on installing the WebLogic Server, refer to *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

  - Oracle SOA Suite installed and patched to at least PS2

    For information on installing the Oracle SOA Suite, refer to *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

  - Oracle HTTP Server installed

    For information on installing Oracle HTTP Server, refer to *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*.

- Oracle Access Manager 10*g* or 11*g* agent (WebGate) for Oracle HTTP Server 11*g* must be installed on the Oracle HTTP Server 11*g* instance.

  For information on installing the Oracle HTTP Server WebGate, refer to *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

The steps below are based on the assumption that Oracle Access Manager and Oracle Identity Manager are integrated using the out-of-the box integration.

7.4 Overview of Integration Tasks

The following tasks are required to perform this integration:

- Install Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager
- Perform Post-Configuration for Oracle Access Manager and Oracle Adaptive Access Manager
- Register the 11g WebGate
- Integrate Oracle Access Manager and Oracle Identity Manager
- Enable LDAP Synchronization for Oracle Identity Manager
- Integrate Oracle Access Manager and Oracle Adaptive Access Manager
- Integrate Oracle Identity Manager and Oracle Adaptive Access Manager
- Configure Oracle Identity Manager Properties for the Integration
- Configure TAP Scheme to Access Applications in the IAMSuite Agent Application Domain

7.5 Install Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager

Install Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager on different WebLogic servers with Oracle Access Manager and Oracle Adaptive Access Manager in the same or different WebLogic domains.

Note: In this chapter, `OAM_HOME` is `OAM_WL_HOME/Oracle_IDM1`, and `OAAM_HOME` is `OAAM_WL_HOME/Oracle_IDM1`.

For both Oracle Access Manager and Oracle Adaptive Access Manager, ensure that you have:

- Installed the database
- Installed and ran RCU to create database schemas for Oracle Access Manager and Oracle Adaptive Access Manager

For the setup and configuration of Oracle Access Manager, ensure that you have:

- Installed the Oracle WebLogic Server at `OAM_WL_HOME`
- Installed Oracle Access Manager
- Configured Oracle Access Manager

For the setup and configuration of Oracle Adaptive Access Manager, ensure that you have:

- Installed the Oracle WebLogic Server at `OAAM_WL_HOME`
- Installed Oracle Adaptive Access Manager
- Configured Oracle Adaptive Access Manager

Note: If so preferred, Oracle Access Manager and Oracle Adaptive Access Manager can be installed in different domains or on the same WebLogic domain.

For multiple domain installation, the oaam.csf.useMBeans property must be set to true. Refer to "Oracle Adaptive Access Manager Command-Line Interface Scripts" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager* for information on setting this parameter.

During the integration steps below, for reference we will refer to the WLS Domain which contains Oracle Access Manager as `OAM_DOMAIN_HOME`, and the WLS Domain which contains OAAM as `OAAM_DOMAIN_HOME`.

For information on installing the Identity Management Suite, refer to *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

7.6 Perform Post-Configuration for Oracle Access Manager and Oracle Adaptive Access Manager

This section contains steps to perform post-configuration of Oracle Adaptive Access Manager and to verify that Oracle Access Manager and Oracle Adaptive Access Manager are functional.

7.6.1 Restart the Servers

Before you can perform tasks in this section, ensure that the Oracle Access Manager and Oracle Adaptive Access Manager Administration Consoles and managed servers are running.

7.6.2 Create Users and Import Snapshot for Oracle Adaptive Access Manager

To perform the minimum required steps for Oracle Adaptive Access Manager to be functional, create Oracle Adaptive Access Manager users and import the OAAM Snapshot which contains OAAM policies, dependent components, and configurations.

For the complete set of post-configuration procedures, refer to "Setting Up the Oracle Adaptive Access Manager Environment" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

7.6.2.1 Create Oracle Adaptive Access Manager Users

Before you can access the OAAM Administration Console, you must create administration users.

If protecting the OAAM Administration Console, you must take care of user and group creation in the external LDAP store. For details, see "Creating Users and Groups For Oracle Adaptive Access Manager" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

If not protecting the OAAM Administration Console, then the administration user must be created in the WebLogic Administration Console. To create an administration user in the WebLogic Administration Console:

Note: You can disable OAAM Administration Console protection by disabling the IDM Domain Agent that protects it. To do so, you must set the environment variable or Java property `WLSAGENT_DISABLED=`**true**.

For instructions on disabling the IDM Domain Agent, refer to "Disabling the IDM Domain Agent" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

---

1. Log in to the Oracle WebLogic Administration Console for your WebLogic administration domain.
2. In the Domain Structure tab at the left-hand side, select **Security Realms**.
3. On the Summary of Security Realms page, select the realm that you are configuring (for example, `myrealm`).
4. On the Settings for Realm Name page select **Users and Groups** > **Users**.
5. Click **New** and provide the required information to create a user, such as `user1`, in the security realm:
   - Name: `oaam_admin_username`
   - Description: optional
   - Provider: `DefaultAuthenticator`
   - Password/Confirmation
6. Click the newly created user, `user1`.
7. Click the **Groups** tab.
8. Assign any of the groups with the `OAAM` prefix to the user, `user1`.
9. Click **Save**.

7.6.2.2 Import Oracle Adaptive Access Manager Snapshot

A full snapshot of policies, dependent components and configurations is shipped with Oracle Adaptive Access Manager. For Oracle Adaptive Access Manager to be functional, import the snapshot into the system by following these instructions:

1. Log in to the OAAM Administration Console at the URL:

   `http://`*oaam_managed_server_host*`:`*oaam_admin_managed_server_port*`/oaam_admin`

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

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

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

      A Load and Restore Snapshot dialog appears.

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

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

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

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

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

      The default `oaam_base_snapshot.zip` is located in the *Oracle_IDM1*/oaam/init directory.

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

7.6.3 Set Up Validation for Oracle Access Manager and Oracle Adaptive Access Manager

Once installation and post-installation are completed, check that Oracle Access Manager and Oracle Adaptive Access Manager have been set up correctly by following the instructions in the sections that follow.

7.6.3.1 Validate the Oracle Access Manager Setup

Perform these steps to ensure that Oracle Access Manager is properly configured:

1. Go to `http://`*oam_admin_server_host*`:`*oam_admin_server_port*`/oamconsole`.

   You should be redirected to the Oracle Access Manager Server for login.

2. Provide the administrator user name and password.

   Verify that login to the Oracle Access Manager Administration Console is successful.

7.6.3.2 Validate Oracle Adaptive Access Manager Setup

Try to access the OAAM Server using the URL: `http://`*host*`:`*port*`/oaam_server`. You should be able to log in to the OAAM Server and be able to register a profile.

Note: When you login now, you will need to provide the password as "test" because the Oracle Access Manager and Oracle Adaptive Access Manager integration has not yet been performed. You must change the password immediately after the integration.

7.7 Register the 11*g* WebGate

This section describes how to register the 11*g* WebGate. The WebGate is an out-of-the-box access client. This Web server access client intercepts HTTP requests for Web resources and forwards these to the Oracle Access Manager 11*g* Server.

7.7.1 Pre-requisites for WebGate Registration

Ensure that the following are installed before configuring and registering the Oracle Web Gate:

- WebLogic Server for Oracle HTTP Server (`WLS_FOR_OHS`)
- Oracle HTTP Server (`WLS_FOR_OHS/Oracle_WT1`, call this `OHS_HOME`)
- WebGate (`WLS_FOR_OHS/Oracle_OAMWebGate1`, call this `WG_HOME`)

7.7.2 Configure the 11*g* WebGate

After installing Oracle HTTP Server 11*g* WebGate for Oracle Access Manager, refer to "Post-Installation Steps" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

7.7.3 Register the 11*g* WebGate as a Partner

You must register the Oracle Access Manager Agent that resides on the computer hosting the application to be protected.

Refer to the "Registering and Managing OAM Agents Using the Console" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

1. Register the 11*g* WebGate partner using the Oracle Access Manager Administration Console. For example:

   ```
   11gWG_myhost
   ```

2. Click the **Edit** button in the tool bar to display the configuration page.
3. Set the **Access Client Password** and click **Apply**. Note the Artifacts Location in the confirmation message.
4. In the Artifacts Location, locate the `ObAccessClient.xml` configuration file and `cwallet.sso` and copy them to the *OHS_HOME*`/instances/`*instance*`/config/OHS/`*component*`/webgate/config` directory.

7.7.4 Restart the OHS WebGate

To restart the OHS WebGate issue the following commands:

1. Navigate to the *OHS_HOME*`/instances/`*instance*`/bin` directory.
2. Stop the agent.

```
./opmnctl startall
```

3. Start the agent.

```
./opmnctl startall
```

7.7.5 Validate the WebGate Setup

Once the setup of WebGate is complete, validate the registration:

1. Navigate to `http://ohs_host:ohs_port/`.

   You should be redirected to Oracle Access Manager for authentication.

2. Enter username and password.

   You should see the Oracle HTTP Server Welcome page.

   This is the partner that will be protected using Oracle Adaptive Access Manager.

7.8 Integrate Oracle Access Manager and Oracle Identity Manager

Integration between Oracle Identity Manager and Oracle Access Manager is required for integration between Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager.

For more information, see Chapter 5, "Integrating Oracle Access Manager and Oracle Identity Manager."

7.9 Enable LDAP Synchronization for Oracle Identity Manager

Enabling LDAP synchronization for Oracle Identity Manager is required for integration between Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager.

Oracle Adaptive Access Manager will be working off the same directory with which Oracle Identity Manager is synchronizing.

> **Note:** The UID must match the CN of the newly created user in the LDAP store; otherwise, a login failure occurs.

For information about configuring LDAP synchronization, see the following sections in Chapter 15, "Configuring Oracle Identity Manager" of the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*: "Completing the Prerequitistes for Enabling LDAP Synchronization", "Running the LDAP Post-Configuration Utility", and "Verifying the LDAP Synchronization".

7.10 Integrate Oracle Access Manager and Oracle Adaptive Access Manager

This task involves integrating the Oracle Access Manager and Oracle Adaptive Access Manager components as part of integrating Oracle Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager (OAAM) to deliver password management and challenge-related functionality to Oracle Access Manager-protected applications.

Note: In the integration of Oracle Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager, the IdentityManagerAccessGate profile should already exist since it is configured during the Oracle Access Manager and Oracle Identity Manager integration (see Section 7.8, "Integrate Oracle Access Manager and Oracle Identity Manager").

You configure Oracle Access Manager and Oracle Adaptive Access Manager integration so that the OAAM server acts as a trusted partner application. The OAAM server uses the Trusted Authentication Protocol (TAP) to communicate the authenticated user name to the Oracle Access Manager server after it performs strong authentication, risk, and fraud analysis. In this integration, the Oracle Access Manager server is responsible for redirecting to the protected resource.

Note: For this section:

`OAM_HOME` is `OAM_WL_HOME/Oracle_IDM1`. For referring to Oracle Access Manager Software Install, we use `OAM_HOME`.

`OAAM_HOME` is `OAAM_WL_HOME/Oracle_IDM1`. For referring to Oracle Adaptive Access Manager Software Install, we use `OAAM_HOME`.

During the integration steps below, for reference the WLS Domain which contains Oracle Access Manager is referred to as `OAM_DOMAIN_HOME`, and the WLS Domain which contains Oracle Adaptive Access Manager is referred to as `OAAM_DOMAIN_HOME`.

Configure the Oracle Adaptive Access Manager and Oracle Access Manager integration as follows:

- Configure Oracle Access Manager for Oracle Access Manager and Oracle Adaptive Access Manager Integration
- Validate Oracle Access Manager Configuration
- Configure Oracle Adaptive Access Manager for Oracle Access Manager and Oracle Adaptive Access Manager Integration
- Protect a Resource with Oracle Adaptive Access Manager in Oracle Access Manager
- Validate the Oracle Access Manager and Oracle Adaptive Access Manager Integration

7.10.1 Configure Oracle Access Manager for Oracle Access Manager and Oracle Adaptive Access Manager Integration

If Oracle Access Manager is configured to use the Simple Security Transportation protocol, you must register the OAAM Server as a partner application using the `registerThirdPartyTAPPartner` WLST command.

7.10.1.1 Register the OAAM Server as a Partner Application

To register the OAAM Server as a partner application, follow these steps:

1. Ensure that the OAM Administration Server is running.

2. Set up the environment for WLST.
3. Go to *IAM_ORACLE_HOME*/common/bin.
4. Execute the `wlst.sh` to enter the WLST shell.
5. Connect to the WebLogic Administration Server using the connect command:

   connect ('username', 'password', 't3://hostname:port')

   For example,

   connect("weblogic","admin_password","t3://*AdminHostname*:7001")
6. Execute `registerThirdPartyTAPPartner` WLST.

   An example is provided below.

```
registerThirdPartyTAPPartner(partnerName = "OAAMPartner", keystoreLocation=
"/scratch/jsmith/dwps1tap/TapKeyStore/mykeystore.jks" ,
password="welcome1", tapTokenVersion="v2.0", tapScheme="TAPScheme",
tapRedirectUrl="http://11gWG_myhost.example.com:14300/oaam_
server/oamLoginPage.jsp")
```

Table 7–1 TAP Partner Example

Parameter	Details
partnerName	partnerName is a unique name. If the partner exists in Oracle Access Manager, the configuration will be overwritten.
keystoreLocation	Keystore is an existing location. If the directory path specified is not present, you will get an error. On Windows, the path needs to be escaped. For example: `"C:\\oam-oaam\\tap\\keystore\\store.jks"` The keystore is the outcome of the `registerThirdPartyTAPPartner` command executed in the instructions above. The location will be passed to the command by the user. In the example shown earlier, it was `keystoreLocation= "/scratch/jsmith/dwps1tap/TapKeyStore/mykeystore.jks"`
password	The password is specified to encrypt the keystore. Make a note of the password as you will need it later.
tapTokenVersion	`tapTokenVersion` is always v2.0 for 11.1.1.5.0.
tapScheme	This is the authentication scheme that will be updated. If you want two tap partners with different tapRedirectUrls, create a new authentication scheme using the Oracle Access Manager Administration Console and use that scheme here. The authentication scheme will be created automatically while you are running the `registerThirdPartyTAPPartner` command in the instructions above. The name of the TAP scheme will be passed as parameter to that command. The example command has `tapScheme="TAPScheme"`.
tapRedirectUrl	This URL must work. If it does not work, registration will fail. `tapRedirectUrl` is constructed as follows: `http://`*oaam_server_host*`:`*oaam_server_port*`/oaam_server/oamLoginPage.jsp` This URL should be reachable, otherwise the validation will fail and the partner will not be created. In the Oracle Access Manager and Oracle Adaptive Access Manager integration, the credential collector page will be served by the OAAM Server. The authentication scheme created by `registerThirdPartyTAPPartner` (TAPScheme) points to the OAAM Server credential collector page as the redirectURL.

7.10.1.2 Update the IAMSuite Agent

After generating the initial configuration, you must update the IAMSuite Agent:

1. Log in to the Oracle Access Manager Administration Console.
2. Select the **System Configuration** tab.
3. Select **Access Manager Settings - SSO Agents - OAM Agent** from the directory tree. Double-click or select the open folder icon.
4. Search for **IAMSuiteAgent** and click the entry found in the Search Results.

   The IAMSuiteAgent details page appears.
5. Provide the password for **Access Client Password**.
6. Click **Apply**.

7.10.1.3 Configure for Domain Agent

Note: The IAMSuite Agent is now in **Open Mode** with password authentication. If you are using the Domain Agent in the IDM Domain for another console, make the following change to continue using the Domain Agent.

1. Log in to WebLogic Administration Console.
2. Select **Security Realms** from the Domain Structure menu.
3. Click **myrealm**.
4. Click the **Providers** tab.
5. Select **IAMSuiteAgent** from the list of authentication providers.
6. Click **Provider Specific**.
7. Enter the agent password and type.
8. To confirm, click **Save**.

7.10.2 Validate Oracle Access Manager Configuration

To validate the Oracle Access Manager configuration, perform the following steps:

1. Log in to the Oracle Access Manager Administration Console.
2. Edit the Authentication Scheme that was specified above. This is the value specified for the `tapScheme` parameter.
3. Verify that the `Challenge URL` is set to the value specified in `tapRedirectUrl`. For information on the URL, refer to Table 7–1, " TAP Partner Example".
4. Validate IAMSuiteAgent setup.
5. Launch OAM tester at *OAAM_HOME*/../<jdk160_24>/bin/java -jar *OAAM_HOME*/oam/server/tester/oamtest.jar.
6. Provide server connection details:
   a. IP Address: OAM Managed Server Host
   b. Port: OAM Oracle Access Protocol (OAP) Port
   c. Agent ID: `IAMSuiteAgent`
   d. Agent Password: `Password` provided inUpdate the IAMSuite Agent
   e. Click on **Connect**.

      If you can connect to the server, the next section, **Protected Resource URI**, will be enabled.

7. Provide the protected resource URI as follows:
   a. Host: `IAMSuiteAgent`
   b. Port: `80`
   c. Resource: `/oamTAPAuthenticate`
   d. Click **Validate**

      If the validation is successful, the next section for **User Identity** will be enabled.
8. Provide `User Identity` and click **Authenticate**. If the authentication is successful, the setup is successful.

7.10.3 Configure Oracle Adaptive Access Manager for Oracle Access Manager and Oracle Adaptive Access Manager Integration

Set up the Oracle Access Manager and Oracle Adaptive Access Manager Integration:

1. Copy the OAAM CLI folder to a working directory:

   cp -r *OAAM_HOME*/oaam/cli TEMP/oaam_cli
2. Go to the work folder where you copied the `cli` folder and open `TEMP/oaam_cli/cli/conf/bharosa_properties/oaam_cli.properties` in a text editor and set the properties in Table 7–2.

Table 7–2 OAAM CLI Properties

Parameter	Details
oaam.adminserver.hostname	This is the Admin Server Host of the WebLogic Server Domain where OAAM is installed.
oaam.adminserver.port	This is the Admin Server port of the WebLogic Server Domain where OAAM is installed.
oaam.adminserver.username	This is the Admin Server username of the WebLogic Server Domain (usually weblogic).
oaam.adminserver.password	This is the password of the user specified in oaam.adminserver.username property.
oaam.db.url	This is the valid JDBC URL of the OAAM database in the format: jdbc:oracle:thin:@*db_host*:*db_port*:*db_sid*
oaam.uio.oam.tap.keystoreFile	This is the location of keystore file generated by `registerThirdPartyTAPPartner` WLST. Copy the file from the location specified in the above WLST for parameter "`keystoreLocation`". If Oracle Access Manager and OAAM are on different machines, you will need to manually copy the keystore file created in the OAM server to the OAAM Server and provide the location on the OAAM server here. On Windows, the file path value must be escaped. For example: "`C:\\oam-oaam\\tap\\keystore\]store.jks`"
oaam.uio.oam.tap.partnername	This is the "partnerName" used in the WLST registerThirdPartyTAPPartner command. For example, OAAMPartner.
oaam.uio.oam.host	This is the OAM Primary Host.
oaam.uio.oam.port	This is the OAM Primary NAP (Network Assertion Protocol)/OAP Port. This is the OAM Server port, with the default port number 5575.

Table 7–2 (Cont.) OAAM CLI Properties

Parameter	Details
oaam.uio.oam.webgate_id	This is the `IAMSuiteAgent` value. Do NOT change this.
oaam.uio.oam.secondary.host	This is the OAM Secondary Host.
oaam.uio.oam.secondary.host.port	This is the OAM Secondary NAP/OAP Port.

3. Set the environment variable `ORACLE_MW_HOME` to the location of the WebLogic Server install where Oracle Adaptive Access Manager is installed.

   ```
   setenv ORACLE_MW_HOME <Location of WLS install where Oracle
   Adaptive Access Manager is installed>
   ```

4. Set the environment variable `JAVA_HOME` to the JDK used for the WebLogic installation.
5. Run the following command:

   ```
   TEMP/oaam_cli/cli/setupOAMTapIntegration.sh TEMP/oaam_
   cli/cli/conf/bharosa_properties/oaam_cli.properties
   ```

7.10.4 Protect a Resource with Oracle Adaptive Access Manager in Oracle Access Manager

To protect a resource with Oracle Adaptive Access Manager, follow these steps:

1. Log in to the Oracle Access Manager Administration Console.
2. Check for the Application Domain that was created as part of the 11gWebGate registration. (**11gWG_myhost** in the example).
3. Edit the Authentication Policy, following these steps:
   a. From the Navigation window expand: **Application Domains** > **11gWG_myhost** > **Authentication Policies**.
   b. Click **Protected Resource Policy**.

      Except for "11gWG_myhost" in the example, all other strings would be as is in Oracle Access Manager.

   c. Update **Authentication Scheme** to the TAP scheme specified as the "`tapScheme`" parameter in "`registerThirdPartyTAPPartner`" command.
4. Click **Apply** to save the changes.

7.10.5 Validate the Oracle Access Manager and Oracle Adaptive Access Manager Integration

Try to access the protected resource. You should be redirected to OAAM for registration and challenge. The OAAM login page is shown instead of the Oracle Access Manager login page.

7.11 Integrate Oracle Identity Manager and Oracle Adaptive Access Manager

This section describes how to integrate Oracle Identity Manager and Oracle Adaptive Access Manager for the three-way integration of Oracle Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager:

- Set Oracle Adaptive Access Manager Properties for Oracle Identity Manager
- Set Oracle Identity Manager Credentials in Credential Store Framework

7.11.1 Set Oracle Adaptive Access Manager Properties for Oracle Identity Manager

To set Oracle Adaptive Access Manager properties for Oracle Identity Manager:

1. Go to the OAAM Administration Console at the URL:

   `http://`*oaam_managed_server_host*`:`*oaam_admin_managed_server_port*`/oaam_admin`

2. Log in as a user with access to the Properties Editor.
3. Open the Oracle Adaptive Access Manager Property Editor to set the Oracle Identity Manager properties.

   If a property does not exist, you need to add it.

   For the following properties, set the values according to your deployment:

Table 7–3 Configuring Oracle Identity Manager Property Values

Property Name	Property Values
bharosa.uio.default.user.management.provider.classname	`com.bharosa.vcrypt.services.OAAMUserMgmtOIM`
oaam.oim.auth.login.config	`${oracle.oaam.home}/../designconsole/config/authwl.conf`

oaam.oim.url	`t3://<OIM Managed Server>:<OIM Managed Port>`
	For example, `t3://host.example.com:14000`
	URLs can be listed as comma-separated values; for example:
	`oaam.oim.url = t3://oimhost1.mycompany.com:14000,oimhost2.mycompany.com:14000`
	The two OIM hosts are clustered and load balanced, however there's no hardware load-balancer to route the traffic between them. In this case, if one of the hosts is down, the traffic is routed to the other.

oaam.oim.xl.homedir	${oracle.oaam.home}/../designconsole
bharosa.uio.default.signon.links.enum.selfregistration.url	`http://<OIM Managed Server>:<OIM Managed Port>/oim/faces/pages/USelf.jspx?E_TYPE=USELF&OP_TYPE=SELF_REGISTRATION&backUrl=<OAAM Login URL for OIM>` where `<OAAM Login URL for OIM>` is `http://<OHS host>:<OHS port>/oim/faces/pages/Self.jspx` or (in case of IDMDOMAINAgent) is `http://<OIM host>:<OIMport>/oim/faces/pages/Self.jspx`. OHS setup was performed during the integration between Oracle Access Manager and Oracle Identity Manager.

Table 7–3 (Cont.) Configuring Oracle Identity Manager Property Values

Property Name	Property Values
bharosa.uio.default.signon.links.enum.trackregistration.url	`http://<OIM Managed Server>:<OIM Managed Port>/oim/faces/pages/USelf.jspx?E_TYPE=USELF&OP_TYPE=UNAUTH_TRACK_REQUEST&backUrl=<OAAM Login URL for OIM>` where `<OAAM Login URL for OIM>` is `http://<OHS host>:<OHS port>/oim/faces/pages/Self.jspx` or (in case of IDMDOMAINAgent) is `http://<OIM host>:<OIMport>/oim/faces/pages/Self.jspx`. OHS setup was performed during the integration between Oracle Access Manager and Oracle Identity Manager.
bharosa.uio.default.signon.links.enum.trackregistration.enabled	true
bharosa.uio.default.signon.links.enum.selfregistration.enabled	true
oaam.oim.csf.credentials.enabled	true This property enables the configuring of credentials in the Credential Store Framework as opposed to maintaining them using the Properties Editor. This step is performed so that credentials can be securely stored in CSF.

For information on setting properties in Oracle Adaptive Access Manager, see "Using the Property Editor" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

7.11.2 Set Oracle Identity Manager Credentials in Credential Store Framework

So that Oracle Identity Manager WebGate credentials can be securely stored in the Credential Store Framework, follow these steps to add a password credential to the Oracle Adaptive Access Manager domain:

1. Go to the Oracle Fusion Middleware Enterprise Manager Console at `http://`*weblogic_host*`:`*administration_port*`/em`.
2. Log in as a WebLogic Administrator, for example `WebLogic`.
3. Expand the **<Base_Domain>** icon in the navigation tree in the left pane.
4. Select your domain name, right click, and select the menu option **Security** and then the option **Credentials** in the sub menu.
5. Click **Create Map**.
6. Click **oaam** to select the map, then click **Create Key**.
7. In the pop-up dialog, ensure that **Select Map** is **oaam**.
8. Provide the following properties and click **OK**.

Table 7–4 Oracle Identity Manager Credentials

Name	Value
Map Name	`oaam`
Key Name	`oim.credentials`

Table 7–4 (Cont.) Oracle Identity Manager Credentials

Name	Value
Key Type	Password
UserName	Username of Oracle Identity Manager Administrator
Password	Password of Oracle Identity Manager Administrator

7.12 Configure Oracle Identity Manager Properties for the Integration

In Oracle Identity Manager, system properties are configured to enable Oracle Adaptive Access Manager instead of Oracle Identity Manager to provide the functionality related to challenge questions.

To modify Oracle Identity Manager properties for Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager integration, take these steps:

1. Log in to the Oracle Identity Manager Administrative Console.
2. Click the **Advanced** link in the self-service console.
3. Click **System Properties** in **System Management**.
4. Click on **Advanced Search**.
5. Set the following properties and click **Save**.

> **Note:** For the URLs, use the hostnames as they were configured in Oracle Access Manager. For example, if a complete hostname (with domain name) was provided during Oracle Access Manager configuration, use the complete hostname for the URLs.

Table 7–5 Oracle Identity Manager Redirection

Keyword	Property Name and Value
OIM.DisableChallengeQuestions	TRUE
OIM.ChangePasswordURL	URL for change password page in Oracle Adaptive Access Manager (http://*oaam_server_managed_server_host*:*oaam_server_managed_server_port*/oaam_server/`oimChangePassword.jsp` In a high availability (HA) environment, set this property to point to the virtual IP URL for the OAAM server.
OIM.ChallengeQuestionModificationURL	URL for challenge questions modification page in Oracle Adaptive Access Manager (http://*oaam_server_managed_server_host*:*oaam_server_managed_server_port*/`oaam_server/oimResetChallengeQuestions.jsp`)

7.13 Configure TAP Scheme to Access Applications in the IAMSuite Agent Application Domain

> **Note:** The instructions in this section should only be performed if you want to use the TAP Scheme in the IAMSuiteAgent application domain.

To use TAP scheme for Identity Management product resources in the IAM Suite domain, Protected HigherLevel Policy, the following configuration must be performed:

1. Log in to the Oracle Access Manager Administration Console.
2. Navigate to **Policy Configuration**, select **Application Domains**, select **IAMsuiteAgent**, select **Authentication Policies**, and select **Protected Higher Level Policy**.
3. On the Authentication Policy page, remove `IAMSuiteAgent:/oamTAPAuthenticate` from the Resources tab.
4. Click **Apply**.
5. Create a new Authentication Policy in the IAMSuite Application Domain.
6. On the Authentication Policy page, select `LDAPScheme` in the **Authentication Scheme** field.
7. Add `IAMSuiteAgent:/oamTAPAuthentication` as a resource.
8. Click **Apply**.

7.14 Troubleshooting Tips

This section provides additional troubleshooting and configuration tips for the integration of Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager.

7.14.1 Policies and Challenge Questions

You may encounter a non-working URL if policies and challenge questions are not available as expected in your Oracle Adaptive Access Manager environment. For example, the Forgot Password page will fail to come up and you are redirected back to the login page.

To ensure correct operation, make sure that the default base policies and challenge questions shipped with Oracle Adaptive Access Manager have been imported into your system. For details, see Setting Up the Oracle Adaptive Access Manager Environment in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

7.14.2 Cookie Domain Definition

Incorrect value of the cookie domain in your configuration can result in login failure.

For correct WebGate operation, ensure that the property `oaam.uio.oam.obsso_cookie_domain` is set to match the corresponding value in Oracle Access Manager; for example, `.us.example.com`.

7.14.3 In the OAM and OAAM Integration TAP Could Not Modify User Attribute

In integration scenarios coupled with multiple identity stores, the user identity store that is set as the Default Store is used for authentication and assertion. If you change the Default Store to point to a different store, ensure that the TAPScheme also points to same store.

For the OAM-OAAM TAP integration, the assertion for the TAPScheme Authentication Scheme is made against the Default Store. In this case the backend channel authentication made against the LDAP module uses a specific user identity store (OID, for example). When the username is returned to Oracle Access Manager, the assertion occurs against the Default Store (not the same OID that was used for the authentication).

> **Note:** For Session Impersonation, the Oracle Internet Directory instance that is used for the user and grants must be the Default Store.

If you change the Default Store, ensure that the TAPScheme also points to same store. Otherwise, authentication can succeed but the final redirect can fail with the following errors:

```
Module oracle.oam.user.identity.provider
Message Principal object is not serializable; getGroups call will result in
an extra LDAP call

Module oracle.oam.engine.authn
Message Cannot assert the username from DAP token

Module oracle.oam.user.identity.provider
Message Could not modify user attribute for user : cn, attribute :
userRuleAdmin, value : {2} .
```

7.14.4 TAP: setupOAMTapIntegration Script Does Not Provide Exit Status Message

When the `setupOAMTapIntegration` script is run to configure Oracle Adaptive Access Manager for Oracle Access Manager and Oracle Adaptive Access Manager integration, a message is not provided to indicate whether the script completed successfully or failed.

8

Integrating Oracle Access Manager 10*g* and Oracle Adaptive Access Manager 11*g*

This chapter describes the process for integrating Oracle Adaptive Access Manager 11*g* with Oracle Access Manager 10*g*. The integration works as follows:

1. When the user tries to access a protected resource, he is redirected to the Oracle Adaptive Access Manager login page instead of the Oracle Access Manager login.
2. Oracle Adaptive Access Manager delegates user authentication to Oracle Access Manager.
3. Then, Oracle Adaptive Access Manager performs risk analysis of the user.

This chapter contains these sections:

8.1 Prerequisites

Ensure that the following prerequisites are met before performing the integration:

- All necessary components have been properly installed and configured:
  - Oracle Adaptive Access Manager 11*g*
  - Oracle Access Manager 10.1.4.3
  - Application Server
- The Oracle Access Manager environment has been configured to protect simple HTML resources using two different authentication schemes:

- The first authentication scheme uses Basic Over LDAP.
- The second authentication scheme is a higher-security level and integrates OAAM Server by using a custom form-based authentication scheme.

  Refer to Section 8.4, "Configure OAM Authentication Scheme.".

8.2 Integration Overview

Except where specified, the following procedures are required to complete the integration of Oracle Access Adaptive Manager 11*g* and Oracle Access Manager 10*g*.

- Configure OAM AccessGate for OAAM Web Server
- Configure OAM Authentication Scheme
- Configure Oracle Access Manager Connection (Optional)
- Set Up WebGate for OAAM Web Server
- Configure OAM Domain to Use OAAM Authentication
- Configure OHS
- Configure Oracle Adaptive Access Manager Properties
- Turn Off IP Validation

8.3 Configure OAM AccessGate for OAAM Web Server

In Oracle Access Manager and Oracle Adaptive Access Manager integration, the Oracle Access Manager AccessGate fronts the Web server (a traditional WebGate) to OAAM Server.

To configure the Oracle Access Manager AccessGate that fronts the Web server to OAAM Server, perform the following steps:

1. Click **Add New AccessGate**.
2. Use the settings in the table below to create a new AccessGate and assign it an Access Server

Table 8–1 OHS WebGate Configuration

Parameter	Value
AccessGate Name	ohsWebGate
Description	AccessGate for Web server hosting OAAM Server
Hostname	<hostname>
Port	<port>
AccessGate Password	<passwd>
Debug	<Off>
Maximum user session time (seconds)	3600
Idle Session Time (seconds)	3600
Maximum Connections	1
Transport Security	<Open>

Table 8–1 (Cont.) OHS WebGate Configuration

Parameter	Value
IP Validation	<On>
IP Validation Exception	<leave blank>
Maximum Client Session Time (hours)	24
Failover Threshold	1
Access server timeout threshold	<leave blank>
Sleep for (seconds)	60
Maximum elements in cache	10000
Cache timeout (seconds)	1800
Impersonation Username	<leave blank>
Impersonation Password	<leave blank>
Access Management Service	<On>
Preferred HTTP Cookie Domain	.<domain_name>
Preferred HTTP Host	<hostname>:<port>
Deny on not protected	<Off>
CachePragmaHeader	no-cache
CacheControlHeader	no-cache
LogOutURLs	<leave blank>
User Defined Parameters	<leave blank>
Assign An Access Server (Primary)	<oam_hostname>:<port>
Number of Connections	1

3. Click **AccessGate Configuration**.
4. Click **OK** to search for all AccessGates.

   The new AccessGate is now listed

8.4 Configure OAM Authentication Scheme

To leverage OAAM Server as an authentication mechanism, Oracle Access Manager must have a defined Authentication Scheme to understand how to direct authentications to OAAM Server.

To define the authentication scheme for Oracle Adaptive Access Manager, follow the steps below:

1. Click **Authentication Management**.
2. Click **New**.

3. Using the settings in the table below, begin creating the new OAAM Server authentication scheme:

Table 8–2 OAAM Server Authentication Scheme Configuration

Parameter	Value
Name	Adaptive Strong Authentication
Description	Oracle Adaptive Access Manager-OAAM Server virtual authentication pad authentication scheme
Level	3
Challenge Method	Form
Challenge Parameter(s)	form:/oaam_server/oamLoginPage.jsp
	creds:userid password
	action:/oaam_server/
SSL Required	<No>
Challenge Redirect	<Redirect Url>
Enabled	<Disabled/Greyed Out>

4. Click **Save**.
5. Click **Ok** to confirm the saved operation.
6. Click **Plugins**.
7. Click **Modify**.
8. Click **Add**.
9. Create the plugin configurations using the information presented in the table below.

Table 8–3 OAAM Server Authentication Scheme Configuration - Plugins

Plugin Name	Plugin Parameters
credential_mapping	obMappingBase="dc=<domain>,dc=com",obMappingFilter="(uid=%userid%)"
validate_password	obCredentialPassword="password"

10. Click **Save**.
11. Click **General**.
12. Click **Modify**.
13. Set **Enabled** to **Yes**.
14. Click **Save**.

8.5 Configure Oracle Access Manager Connection (Optional)

The AccessGates used by OAAM Server must have host identifier entries. Use the Host Identifiers feature to enter the official name for the host, and every other name by which the host can be addressed by users.

A request sent to any address on the list is mapped to the official host name, and applicable rules and policies are implemented. This is primarily used in virtual site hosting environments.

8.6 Set Up WebGate for OAAM Web Server

To correctly handle the cookies for authentication and the required HTTP headers for the OAAM Server, OAAM Server must be protected with a standard WebGate and Web server.

To set up the WebGate for use with OAAM Server, follow these steps:

1. Install an Apache HTTP server 2.x and configure it with the WebLogic Server Plug-in.

   For instructions on installing and configuring the Apache HTTP Server Plug-In, refer to the document named *Oracle Fusion Middleware Using Web Server 1.1 Plug-Ins with Oracle WebLogic Server*.

2. Stop the application server (and Web server).
3. Run the WebGate installation program.
4. For the WebGate configuration, use the following settings:

Table 8–4 Setting Up the WebGate for Use with OAAM Server

Attribute	Value
WebGate ID	ohsWebGate
Password for WebGate	<password>
Access Server ID	<Access ServerId>
Host Name	<hostname>
Port	<port

8.7 Configure OAM Domain to Use OAAM Authentication

The OAAM Server authentication should now be operable for Oracle Access Manager policy domains.

To modify the Oracle Access Manager policy domain to use the OAAM authentication scheme (Strong Authentication), follow these steps:

1. Log in to the Oracle Access Manager host. For example, http://*hostname*/access/oblix.
2. Click **Policy Manager**.
3. Log in as an administrator.
4. Click **My Policy Domains**.
5. Click **<ApplicationPolicy >**.
6. Click **Default Rules**.
7. Click **Modify**.
8. From the Authentication Scheme drop-down selector, select **Adaptive Strong Authentication**.
9. Click **OK** to confirm the change in authentication schemes.

10. Ensure that **Update Cache** is checked.
11. Click **Save**.
12. Close Internet Explorer.

8.8 Configure OHS

Configure OHS such that it proxies OAAM server. In 11*g* OHS, that is done by modifying `mod_wl_ohs.conf`.

To setup proxy, you need to go to the OHS `config` folder and modify the `mod_wl_ohs.conf` file. An example of an entry to add is shown below:

```
<Location /oaam_server>
SetHandler weblogic-handler
WebLogicHost name.mycompany.com
WebLogicPort 24300
</Location>
```

8.9 Configure Oracle Adaptive Access Manager Properties

Setting Oracle Adaptive Access Manager properties for Oracle Access Manager and Oracle Access Manager credentials in CSF is required for this integration to work.

8.9.1 Set Oracle Adaptive Access Manager Properties for Oracle Access Manager

Note: Before doing this procedure, you must take into account whether the OAAM Admin Console is being protected.

- If protecting the console, you must take care of user and group creation in the external LDAP store. For details, see Creating Oracle Adaptive Access Manager Administrative Groups and User in LDAP in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

  OR

- If not protecting the OAAM Admin Console, then the user must be created in the WebLogic Administration Console.

  (Note: You can disable OAAM Admin Console protection by setting the environment variable or Java property WLSAGENT_DISABLED=true.)

To set Oracle Adaptive Access Manager properties for Oracle Access Manager:

1. Start the managed server hosting the Oracle Adaptive Access Manager server.
2. Navigate to the Oracle Adaptive Access Manager Admin Console at http://*oaam_managed_server_host*:*oaam_admin_server_port*/oaam_admin.
3. Log in as a user with access to the property editor.
4. Open the Oracle Adaptive Access Manager property editor to set the Oracle Access Manager properties.

   If a property does not exist, you must add it.

For the following properties, set the values according to your deployment:

Table 8–5 Configuring Oracle Access Manager Property Values

Property Name	Property Values
bharosa.uio.default.password.auth.provider.classname	com.bharosa.vcrypt.services.OAMOAAMAuthProvider
bharosa.uio.default.is_oam_integrated	true
oaam.uio.oam.host	Access Server host machine name For example, host.example.com
oaam.uio.oam.port	Access Server Port; for example, 3004
oaam.uio.oam.obsso_cookie_domain	Cookie domain defined in Access Server WebGate Agent
oaam.uio.oam.java_agent.enabled	Default value is false. Set this to true only if the OAM Java Agent (also known as the WLSAgent) is used to protect the application. When setting this property, note the following points about the property oaam.uio.oam.obsso_cookie_name: ■ By default, the property oaam.uio.oam.obsso_cookie_name does not exist. ■ If using Java agent, when setting oaam.uio.oam.java_agent.enabled to true, also set the property oaam.uio.oam.obsso_cookie_name to the value OAMAuthnCookie since the Java agent uses the OAMAuthnCookie cookie. ■ If using WebGate Agent and oaam.uio.oam.java_agent.enabled is set to false, if the property oaam.uio.oam.obsso_cookie_name happens to be set, remove that property. Setting this property is only required when using the OAM Java agent.
oaam.uio.oam.virtual_host_name	Default value is IDMDomain when the OAM Java Agent (also known as the WLSAgent) is used. Change this value only if the virtual host name is different from IDMDomain.
oaam.uio.oam.webgate_id	IdentityManagerAccessGate The name of the WebGate Agent for Oracle Identity Manager integration. The default is IdentityManagerAccessGate.
oaam.uio.login.page	/oamLoginPage.jsp
oaam.uio.oam.authenticate.withoutsession	false

Table 8–5 (Cont.) Configuring Oracle Access Manager Property Values

Property Name	Property Values
oaam.uio.oam.secondary.host	Name of the secondary Access Server host machine. The property must be added, as it is not set by default. This property is used for high availability. You can specify the fail-over hostname using this property.
oaam.uio.oam.secondary.host.port	Port number of the secondary Access Server The property must be added as it is not set by default. This property is used for high availability. You can specify the fail-over port using this property.
oaam.oam.csf.credentials.enabled	true This property enables configuring credentials in the Credential Store Framework instead of maintaining them using the properties editor. This step is performed so that credentials can be securely stored in CSF.

For information on setting properties in Oracle Adaptive Access Manager, see "Using the Property Editor" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

For more information about the IDM Domain Agent, see Section 1.2, "A Note About IDMDomain Agents and WebGates".

8.9.2 Set Oracle Access Manager Credentials in Credential Store Framework

So that Oracle Access Manager WebGate credentials can be securely stored in the Credential Store Framework, follow these steps to add a password credential to the Oracle Adaptive Access Manager domain:

1. Navigate to the Oracle Fusion Middleware Enterprise Manager Console at http://*weblogic_server_host*:*admin_port*/em.
2. Log in as a WebLogic Administrator.
3. Expand **Base_Domain** in the navigation tree in the left pane.
4. Select your domain name, right-click, select the menu option **Security**, and then select the option **Credentials** in the sub-menu.
5. Click **Create Map**.
6. Click oaam to select the map, then click **Create Key**.
7. In the pop-up window make sure Select Map is **oaam**.
8. Provide the following properties and click **OK**.

Table 8–6 Adding Password Credentials to OAAM Domain

Name	Value
Map Name	oaam
Key Name	oam.credentials
Key Type	Password
UserName	Oracle Access Manager user with Administrator rights
Password	Password of Oracle Access Manager WebGate Agent

8.10 Turn Off IP Validation

In order for Oracle Adaptive Access Manager to direct the user to the protected URL after authentication, you must turn off IP validation.

To turn off IP validation, follow the steps below:

1. On the Access System main page, click the **Access System Console** link, and then log in as an administrator.
2. On the Access System Console main page, click **Access System Configuration**, and then click the **Access Gate Configuration** link on the left pane to display the AccessGates Search page.
3. Enter the proper search criteria and click **Go** to display a list of AccessGates.
4. Select the AccessGate.

   For example, **oaam11gWg**.
5. Click **Modify** at the bottom of the page.
6. Set **IP Validation** to **off**.
7. Click **Save** at the bottom of the page.

8.11 Testing Oracle Adaptive Access Manager and Oracle Access Manager Integration

To test the configuration, try accessing your application. The Oracle Access Manager will intercept your un-authenticated request and redirect you to the OAAM Server to challenge for credentials.

9

Configuring Oracle Access Manager For Windows Native Authentication

Oracle Access Manager 11*g* interoperates with Windows Native Authentication (WNA). This chapter explains how to integrate with WNA.

This chapter contains these sections:

9.1 Before You Begin

A fully-configured Microsoft Active Directory authentication service should be set up with user accounts to map Kerberos services, Service Principal Names (SPNs) for those accounts, and key tab files. For more information, see *Oracle Fusion Middleware Securing Oracle WebLogic Server 11g* Release 1 (10.3.3) E13707-03.

See Also: Section 9.3, "Performing Prerequisite Tasks"

9.2 About Oracle Access Manager with Windows Native Authentication

Oracle Access Manager enables Microsoft Internet Explorer users to automatically authenticate to their Web applications using their desktop credentials. This is known as Windows Native Authentication (WNA).

Cross-platform authentication is achieved by emulating the negotiate behavior of native Windows-to-Windows authentication services that use the Kerberos protocol. In order for cross-platform authentication to work, non-Windows servers (in this case, Oracle Access Manager) must parse SPNEGO tokens in order to extract Kerberos tokens which are then used for authentication.

With Oracle Access Manager single sign-on combined with WNA, a Kerberos session ticket is generated that contains her login credentials, among other things. This Kerberos session ticket is not visible to the user.

However, with WNA implemented, the user can click on her Web application without another challenge for credentials. Instead, her Kerberos session ticket, which includes her credentials, is passed through the browser to the Oracle Access Manager server. The server validates the credentials by checking them against the Key Distribution Center server (KDC server) on the Windows domain server. (*Note*: The KDC, which is a trusted third party, uses logically separate servers to grant and process tickets, including the service server to authenticate session tickets and confirm the client's identity.)

If authentication succeeds she is granted access to her Web applications automatically.

For instance, the application must be protected by an Oracle Access Manager application domain that uses the Kerberos authentication scheme (KerbScheme) with WNA as the challenge method. In this case, credentials must be stored in a Windows Active Directory instance that is registered as a user-identify store with Oracle Access Manager.

9.3 Performing Prerequisite Tasks

The integration tasks are as follows:

- Edit the krb5.conf File
- Create the Service Principal Name (SPN)
- Obtain the Kerberos Ticket

9.3.1 Edit the krb5.conf File

To edit the krb5.conf file

1. Open the `krb5.conf` file, which is located in `/etc/krb5.conf`.
2. Update the file with the following entries

```
[Libdefaults]
default_realm = HOLMIUM.NGAM.COM
ticket_lifetime = 600

[realms]

HOLMIUM.NGAM.COM = {
kdc = holmium.us.example.com
admin_server = holmium.us.example.com
default_domain = HOLMIUM.NGAM.COM
}

[domain_realm]
.holmium.ngam.com = HOLMIUM.NGAM.COM
holmium.ngam.com = HOLMIUM.NGAM.COM
```

9.3.2 Create the Service Principal Name (SPN)

You perform this task to create an SPN and associate it with a user.

The following procedure includes an example user named `testuser`. The Oracle Access Manager server is deployed on a machine named `mynode47.us.example.com`.

To create the SPN and associate it with a user

1. Create the user in Microsoft Active Directory.
2. Run `ktpass` to create the service principal name and associate it with this user. For example:

   ```
   ktpass -princ HTTP/service@HOLMIUM.NGAM.COM -pass Oblix!@#
   -mapuser testuser -out D:\etc\ keytab.service
   ```

   Here:

   - HTTP/service@HOLMIUM.NGAM.COM is a principal name associated with user testuser.
   - Oblix!@# is testuser's password.
   - The `service` is the name of the machine on which the Oracle Access Manager server is deployed. For example, if the service is mynode47.us.example.com then the principal name is HTTP/mynode47.us.example.com@HOLMIUM.NGAM.COM.
   - The `-mapuser` parameter specifies a userid (`samaccountname`) to which this principal name is to be attached. A given principal name can only be attached to one user.
   - `D:\etc\ keytab.service` is the keytab file to be generated. Once the file is generated, this keytab file will be used on the Oracle Access Manager server.
3. Copy the newly created `keytab.services` file to the machine on which the NG server is running.

9.3.3 Obtain the Kerberos Ticket

You use the `kinit` command to obtains the master Kerberos ticket that you use to get tickets for other services.

The `kinit` command uses the `/etc/krb5.conf` file; ensure that this file has the correct attributes. The basic syntax for `kinit` is: shown here

```
kinit  [-k] [-t <keytab_filename>] [<principal>]
```

To obtain the Kerberos ticket

1. On the Oracle Access Manager server host machine, run the command from `JDK_HOME/bin`.

   ```
   kinit -V HTTP/mynode47.us.example.com@HOLMIUM.NGAM.COM -k -t
   /scratch/kerberos/keytab.service
   ```

   where:

   - -V indicates verbose mode
   - principal name is HTTP/mynode47.us.example.com@HOLMIUM.NGAM.COM
   - -k instructs the command to use keytab
   - -t is the keytab filename to use

2. Proceed to "Configuring Oracle Access Manager for WNA".

9.4 Configuring Oracle Access Manager for WNA

This section provides the following topics with steps you can follow:

- Set Up the Kerberos Authentication Module in Oracle Access Manager
- Set the Oracle Access Manager Authentication Scheme for Windows Native Authentication
- Register Microsoft Active Directory as a User-Identity Data Store

9.4.1 Set Up the Kerberos Authentication Module in Oracle Access Manager

Before you can use WNA, you must define specific values for the Kerberos authentication module in the Oracle Access Manager policy configuration `oam-policy.xml` file.

Users with valid Oracle Access Manager Administrator credentials can perform the following task to define specific values for the Kerberos authentication module in Oracle Access Manager.

To set up the Kerberos Authentication Module

Note: These instructions require hand-editing a configuration file. You can also perform this task using the OAM Administration Console.

---

1. Locate the `oam-config.xml` file in the following path:

   Middleware_Home/user_projects/domains/IDMDomain/config/fmwconfig/oam-config.xml

2. Make a backup copy of the `oam-config.xml` file and store it in another location in case you need it later.

3. Edit the `oam-config.xml` file to define Kerberos module parameters and values. Examples of these parameters include the keytab file containing pairs of Kerberos principals and encrypted keys, and the krb5.conf file which contains Kerberos configuration information including the locations of KDCs. (*Note*: The files are created at Kerberos installation and appear in the install directory.) Edit the file as follows:

   ```
   <authn-module name="Kerberos" type="KERBEROS" id="4" description="Kerberos
   Module">
   <property value="/u01/app/oracle/install/fmw11g/Middleware/wna/<host_
   name>.keytab" name="keytabfile"/>
   <property value="HTTP/<host_name>.example.com" name="principal"/>
   <property value="/u01/app/oracle/install/fmw11g/Middleware/wna/krb5.conf"
   name="krbconfigfile"/>
   </authn-module>
   ```

   Here, "host_name" is the name of the Oracle Access Manager server host.

4. Save the file.

5. Proceed with "Set the Oracle Access Manager Authentication Scheme for Windows Native Authentication".

9.4.2 Set the Oracle Access Manager Authentication Scheme for Windows Native Authentication

Users with valid Oracle Access Manager administrator credentials can perform the following task to define specific values for the Kerberos authentication module in Oracle Access Manager.

You can use the Oracle Access Manager Administration Console to ensure that the authentication policy for the protected page is set to use the Kerberos authentication scheme and that the scheme uses the Windows Native Authentication challenge method.

To set the Kerberos authentication scheme

1. Configure the Kerberos authentication scheme to use WNA as a challenge method:
   a. From the Oracle Access Manager Policy Configuration tab, navigation pane, expand the Authentication Schemes node.
   b. Double-click KerbScheme to display the configuration details.
   c. Change the Challenge Method to WNA, if needed.
   d. Click Apply and close the confirmation window.
   e. Close the page.
2. Configure the application domain protecting the resource to use the Kerberos authentication scheme as follows:
   a. From the Oracle Access Manager Policy Configuration tab, navigation pane, expand the Application Domains node.
   b. Locate the desired application domain name an expand it.
   c. In the application domain node, expand the Authentication Policies node reveal existing policies.
   d. Double-click your *Protected Resource Policy* to display the related page.
   e. Authentication Scheme: Choose KerbScheme from the list.
   f. Click Apply, and then close the confirmation window.
   g. Close the page.
3. Proceed to "Register Microsoft Active Directory as a User-Identity Data Store".

9.4.3 Register Microsoft Active Directory as a User-Identity Data Store

When using Windows Native Authentication, the user credentials must reside in Microsoft Active Directory, which must be registered as the user identity store for Oracle Access Manager.

Users with valid Oracle Access Manager Administrator credentials can perform the following task to register Microsoft Active Directory as the user store for Oracle Access Manager.

Prerequisites

A fully-configured Microsoft Active Directory authentication service should be set up with User accounts for mapping Kerberos services, Service Principal Names (SPNs) for those accounts, and Key tab files. For more information, see *Oracle Fusion Middleware Securing Oracle WebLogic Server* 11*g* Release 1 (10.3.3).

To register Microsoft Active Directory with Oracle Access Manager

1. From the System Configuration tab, navigation pane, expand the Data Sources node.
2. Click the User Identity Stores node, and then click the Add button in the tool bar.
3. Enter required values for your Microsoft Active Directory. For example:

   Name: *UserIdentityStoreAD*
   LDAP Url: *ldap://ldap_host.domain.com:389*
   Principal: *CN=Administrator,CN=Users,DC=dept,DC=domain,DC=com*
   Credential: ********
   User Search Base: *CN=Users,DC=dept,DC=domain,DC=com*
   User Name Attribute: *UserPrincipalName*
   Subscriber Name: *CN=Users,DC=dept,DC=domain,DC=com*
   LDAP Provider: AD

4. Primary: Click the **Primary** button to make this the primary user identity store for Oracle Access Manager.
5. Role Mapping: By default, the Oracle Access Manager administrator's role is the same as the WebLogic administrator's role (Administrators). However, you can define a new Oracle Access Manager Administrator's role in the primary user identity store for Oracle Access Manager 11*g*. For more information, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.
6. Click **Apply** to submit the changes and dismiss the confirmation window.
7. Restart the Oracle Access Manager Administration Server and managed servers.

9.4.4 Verify the Oracle Access Manager Configuration File

Verify that the following are specified in the `oam-config.xml` file:

- path to the krb5.conf file
- path to the keytab file
- a principal to connect with KDC

Continuing the example used in earlier steps, the `oam-config.xml` file looks as follows:

```
<Setting Name="KerberosModules" Type="htf:map">
   <Setting Name="6DBSE52C" Type="htf:map">
      <Setting Name="principal"
          Type="xsd:string">HTTP/mynode47.us.example.com@HOLMIUM.NGAM.COM
      </Setting>
      <Setting Name="name" Type="xsd:string">XYZKerberosModule</Setting>
      <Setting Name="keytabfile"
          Type="xsd:string">/scratch/kerberos/keytab.service
      </Setting>
      <Setting Name="krbconfigfile" Type="xsd:string">/etc/krb5.conf</Setting>
   </Setting>
</Setting>
```

9.5 Enabling the Browser to Return Kerberos Tokens

You use the following procedures to configure the Internet Explorer or Mozilla Firefox browsers to return Kerberos tokens.

To enable Kerberos tokens in Internet Explorer

1. On a Windows host in the Active Directory domain, sign in as a domain user.
2. Open the Internet Explorer browser.
3. From the Tools menu, click Internet Options, click Security, click Local Intranet, click Advanced.
4. On the Advanced tab, Security section, check the box beside Enable Integrated Windows Authentication, and click OK.
5. Add *Oracle Access Manager CC host or domain name* to Local Intranet zone (use the format `http://mynode.myhost:myport`).
6. Restart the Internet Explorer browser so the change takes affect.

To enable Kerberos tokens in Mozilla Firefox

1. Point the browser to `about:config`.
2. Add *Oracle Access Manager CC host or domain name* under network.negotiate-auth.trusted-uris. Use the format `network.negotiate-auth.trusted-uris=http://mynode.myhost:myport`

9.6 Validating WNA with Oracle Access Manager-Protected Resources

WNA authentication occurs internally.

- The user is redirected to the Oracle Access Manager Server for authentication.
- The Oracle Access Manager Server requests authentication with a www-negotiate header.
- The browser sends the Kerberos SPNEGO token to the Oracle Access Manager Server for authentication.
- The Oracle Access Manager Server authenticates the user's SPNEGO token and redirects the user back to the OSSO Agent or Oracle Access Manager Agent with the cookie and gets access to the resource.

To validate WNA with Oracle Access Manager-protected resources

1. Login to a Windows system in the Active Directory domain as a domain user. Ensure the Internet Explorer is enabled for Integrated Windows Authentication (tools, options, Enable Integrated Windows Authentication, restart the browser).
2. Sign in to the Windows OS client using the Windows domain credentials stored in a hosted Active Directory that is registered with Oracle Access Manager.
3. Start an IE browser, and enter the URL for the OMAM-protected resource.
4. Confirm that access is granted with no additional login.

9.7 Troubleshooting WNA Configuration

Cause

The Identity Store used by Oracle Access Manager might not point to Windows Active Directory. By default, the identity store is Embedded LDAP.

Solution

1. In the Oracle Access Manager Administration Console, review the identity store configuration: System Configuration, Data Sources, User Identity Store.
2. Confirm the LDAP store settings point to Active Directory.

Index

P

S

T

V

W