Oracle® Fusion Middleware

Integration Guide for Oracle Access Manager

11*g* Release 1 (11.1.1)

E15740-02

August 2010

ORACLE®

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

E15740-02

Primary Author: Vinaye Misra

Contributing Author: Priscilla Lee

Contributors: Aarathi Balakrishnan, Gururaj B.S., Sree Chitturi, Toby Close, Ellen Desmond, Gail Flanegin, Don Gosselin, Mark Karlstrand, Ashish Kolli, Svetlana Kolomeyskaya, Madhu Martin, Sergio Mendiola, Vamsi Motukuru, Srinivas Nagandla, Madhan Neethiraj, Rey Ong, Kamal Singh, Saai Soundararajanshanthibai

Contents

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

7 Configuring Oracle Access Manager to use Windows Native Authentication

Index

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/support/contact.html` or visit `http://www.oracle.com/accessibility/support.html` if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Fusion Middleware 11*g* 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* —Describes daily administration and policy configuration tasks using Oracle 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 features and updates.

What's New in 11*g* 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*.

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

1

About Oracle Identity Management Components

This chapter provides an overview of the components with which Oracle Access Manager 11*g* 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*.

1.1 About Oracle Access Manager Integrations

Integrating Oracle Access Manager 11*g* Release 1 (11.1.1) with other applications and portals requires some knowledge of both products. This guide provides the details you need to successfully 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 provided that your webgate uses the IDMDomain preferredHost.
- IDMDomain and WebGate can co-exist. 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*.

1.3 Components Described in This Document

This section provides a brief survey of the Oracle Identity Management components whose integration with Oracle Access Manager is described in this document. They are:

- Oracle Identity Manager
- Oracle Adaptive Access Manager

1.3.1 Oracle Identity Navigator

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 This 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 This component 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 6, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager".

1.3.4 Oracle Adaptive Access Manager

Oracle Adaptive Access Manager This product is Oracle Identity Management's solution for web access real-time fraud detection and multifactor online authentication security for the enterprise. Oracle Adaptive Access Manager consists of two tightly integrated components: Adaptive Strong Authenticator and Adaptive Risk Manager.

For details about integration with Oracle Access Manager, see

- Chapter 5, "Integrating Oracle Access Manager and Oracle Adaptive Access Manager"
- Chapter 6, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager"

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:

> **Note:** Integration procedures are described elsewhere in this document. See Section 2.1, "Summary of Integrations"

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

- Summary of Integrations
- Enabling Identity Administration with Oracle Identity Manager
- Enabling Single Sign-On for Oracle Identity Manager
- Enabling Single Sign-On for Oracle Adaptive Access Manager
- Integrating with Oracle Adaptive Access Manager for Native Authentication
- Enabling Single Sign-On for Oracle Identity Navigator
- Integrating Oracle Access Manager with Oracle Identity Federation
- Integrating Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive Access Manager

2.1 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 2.2, "Enabling Identity Administration with Oracle Identity Manager"
Protecting the Oracle Identity Manager Console	Oracle Identity Manager Oracle Access Manager	Section 2.3, "Enabling Single Sign-On for Oracle Identity Manager"
Protecting the Oracle Adaptive Access Manager Console	Oracle Adaptive Access Manager Oracle Access Manager	Chapter 5, "Integrating Oracle Access Manager and Oracle Adaptive Access Manager"
Protecting the Oracle Identity Navigator Console	Oracle Identity Navigator Oracle Access Manager	Chapter 3, "Integrating with Oracle Identity Navigator"
Pre- and Post-Authentication	Oracle Adaptive Access Manager Oracle Access Manager	Chapter 5, "Integrating Oracle Access Manager and Oracle Adaptive 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 Oracle Access Manager Oracle Identity Manager	Chapter 6, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager"

2.2 Enabling Identity Administration with Oracle Identity Manager

In this release, 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. You can then implement single sign-on for other identity management components and perform additional integrations with suite components, as explained later in this chapter.

The prerequisites for integrating with Oracle Identity Manager are:

- installing the necessary components/suites, which include: RCU, Oracle WebLogic Server, the IAM Suite, and SOA Suite
- creating schemas for Oracle Identity Manager and 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:

- Integration Between OIM and OAM in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- Integrating with Oracle Access Manager in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

2.3 Enabling Single Sign-On for Oracle Identity Manager

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

2.3.1 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

2.3.2 Configuration

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

2.4 Enabling Single Sign-On for Oracle Adaptive Access Manager

You can configure Oracle Access Manager to SSO-enable the Oracle Adaptive Access Manager administration console URL (`/oaam_admin`). In this setup, the OHS proxy for the URL is configured to use 11*g* WebGate.

With this configuration, users enter their credentials on the Oracle Access Manager login page, and are automatically logged into Oracle Adaptive Access Manager.

For configuration details, see Section 5.1, "Protecting the Oracle Adaptive Access Manager Console".

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 5.3, "Native 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 6, "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 11*g* 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
- 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 deployment, these Oracle Adaptive Access Manager and Oracle

Identity Manager secure password collection features 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
- KBA or OTP framework to provide additional authentication when needed
- 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 the rich 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 5, "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 is verified against the identity store using the Oracle Access Manager NAP API. 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, 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 of the processing flow, see Oracle Access Manager Integrated with Oracle Identity Manager

   For implementation details, see Integration Between OIM and OAM in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

2. Oracle Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager integrated for authentication, password management, fraud detection and additional capabilities.

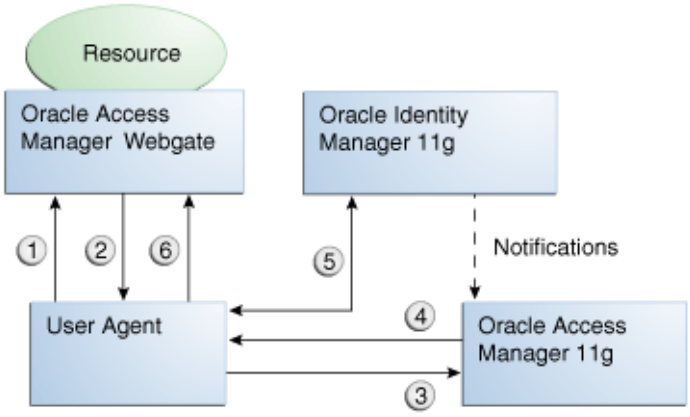
   For details of the processing flow, see Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager Integrated

   For implementation details, see Chapter 6, "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.

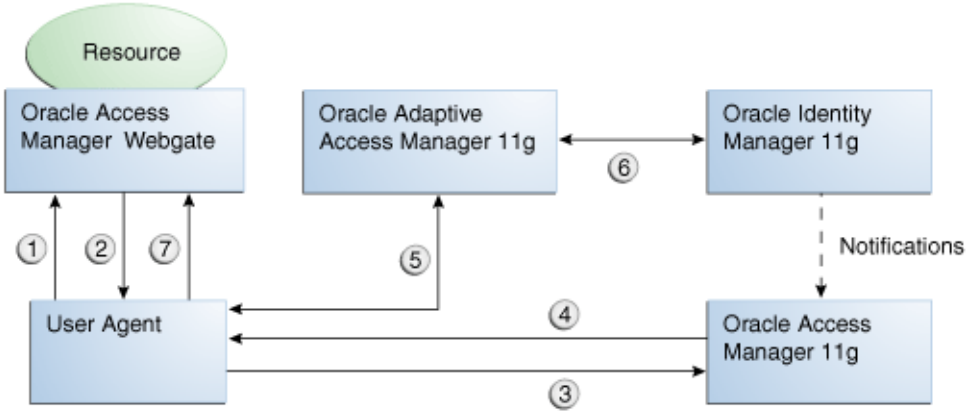
2.8.3.2 Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager Integrated

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 forgot 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.
   - The credentials collected from Oracle Adaptive Access Manager are verified against the identity store by Oracle Access Manager. After validation on the Oracle Access Manager side, 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 over 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 OAM 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 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 an 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
- 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, dynamically 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 the 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 the 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 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.

Note: Oracle Identity Manager does not support automatic locking of a user account after a specific period has elapsed.

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 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 increased 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 the 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. 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. It contains this topic:

- Enabling Single Sign-On

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 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 that is 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 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 the NGAM, 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.

Sections include:

- Background and Integration Overview
- Register Oracle HTTP Server with Oracle Access Manager
- Configure Oracle Identity Federation Providers
- Delegate Authentication to Oracle Identity Federation
- Test the Configuration

4.1 Background and Integration Overview

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

- Overview of Integration Procedure
- Prerequisites
- Additional Setup

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 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

The integration described in this chapter configures Oracle Identity Federation to propagate the authentication state to Oracle Access Manager in SP mode.

In this 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 so that the user can access the requested resource, which is protected by WebGate.

4.1.2 Overview of Integration Procedure

The basic steps required to integrate Oracle Access Manager with Oracle Identity Federation are as follows:

1. Ensure that the necessary components, including Oracle WebLogic Server and Identity Management (IdM) components, are installed.
2. Register Oracle HTTP Server as a partner with the Oracle Access Manager server to protect a resource.
3. Configure the Oracle Identity Federation server to function as a service provider (SP) with Oracle Access Manager.
4. Configure the Oracle Access Manager server to delegate the authentication to Oracle Identity Federation.
5. Test the integration.

The remaining sections provide details about each step.

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*

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

Follow these steps to register Oracle HTTP Server with Oracle Access Manager for authentication:

> **Note:** MW_HOME represents the Oracle Fusion Middleware Home directory.

1. Before registering Oracle HTTP Server with Oracle Access Manager, try accessing the protected resource. For example, if you have the test resource index.html, access it as:

   ```
   http://OHS host:OHS port/private/index.html
   ```

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

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

   Make the necessary changes to the file.

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

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

   Execute the script using this command string:

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

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:

   ```
   <Location /private>
   require valid-user
   AuthType Osso
   </Location>
   ```

7. Restart Oracle HTTP Server.

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

8. Try accessing the protected resource again. You should be redirected to the Oracle Access Manager server for authentication.

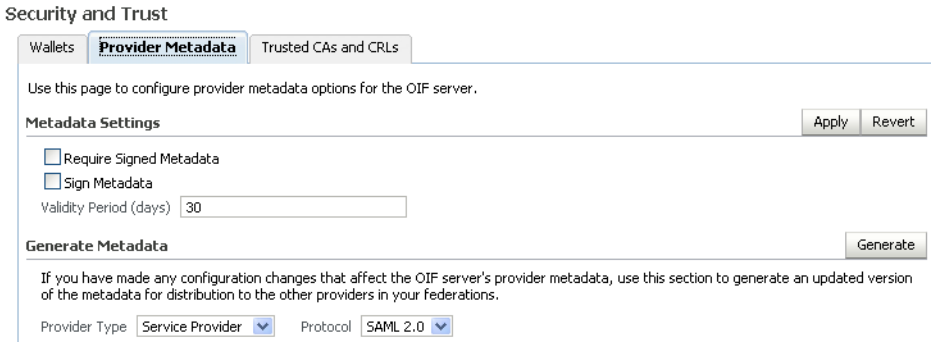
4.3 Configure Oracle Identity Federation Providers

Take these steps to generate and load the metadata for the IdP and SP:

- Generated Provider Metadata
- Register the Providers
- Configure Data Store
- Configure the Authentication Engine
- Set the Default Identity Provider
- Configure Oracle Identity Federation in SP Mode

4.3.1 Generated Provider Metadata

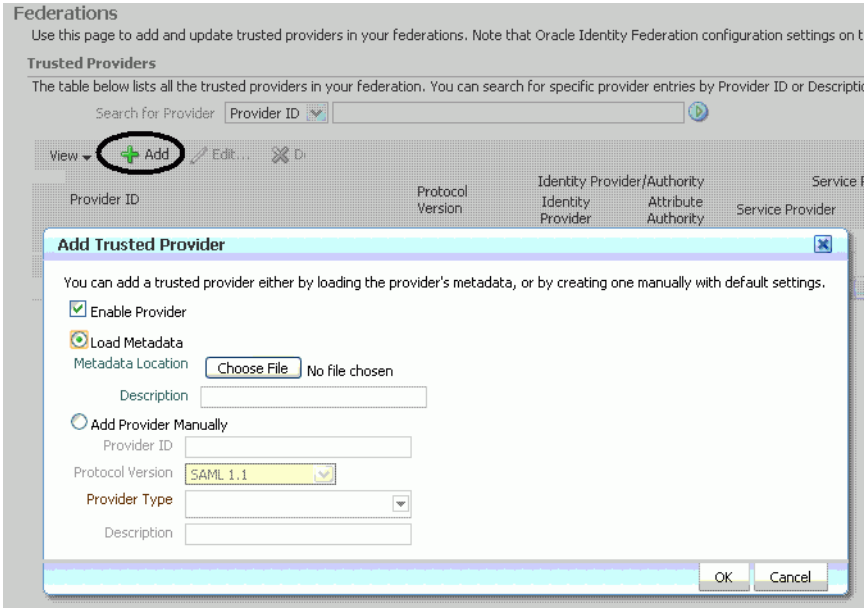
1. Locate the Oracle Identity Federation instance in Fusion Middleware Control.
2. Navigate to **Administration**, then **Security and Trust**.
3. Click the Provider Metadata tab.
4. In the Generate Metadata section of the page, using the Provider Type drop-down, select Service Provider.



5. Click **Generate**. This creates metadata for the service provider.
6. Repeat Steps 4 and 5 to generate metadata for the identity provider.

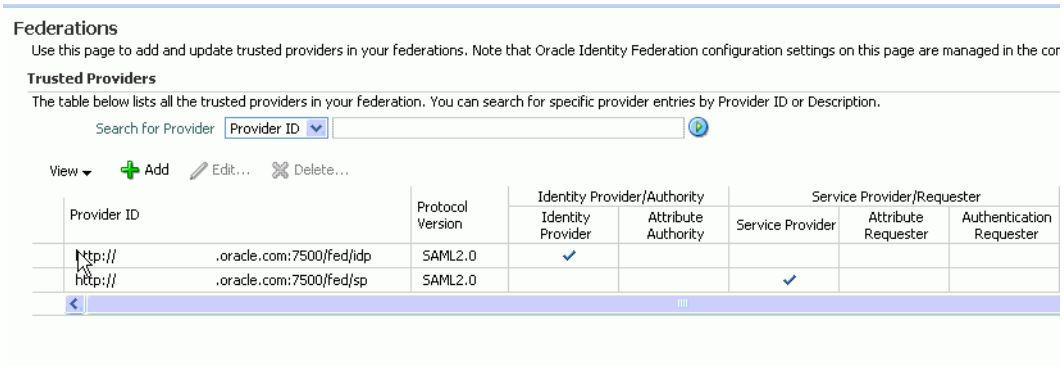
4.3.2 Register the Providers

1. Locate the Oracle Identity Federation instance in Fusion Middleware Control.
2. Navigate to **Administration**, then **Federations**.
3. Click **Add**. The Add Trusted Provider dialog appears.



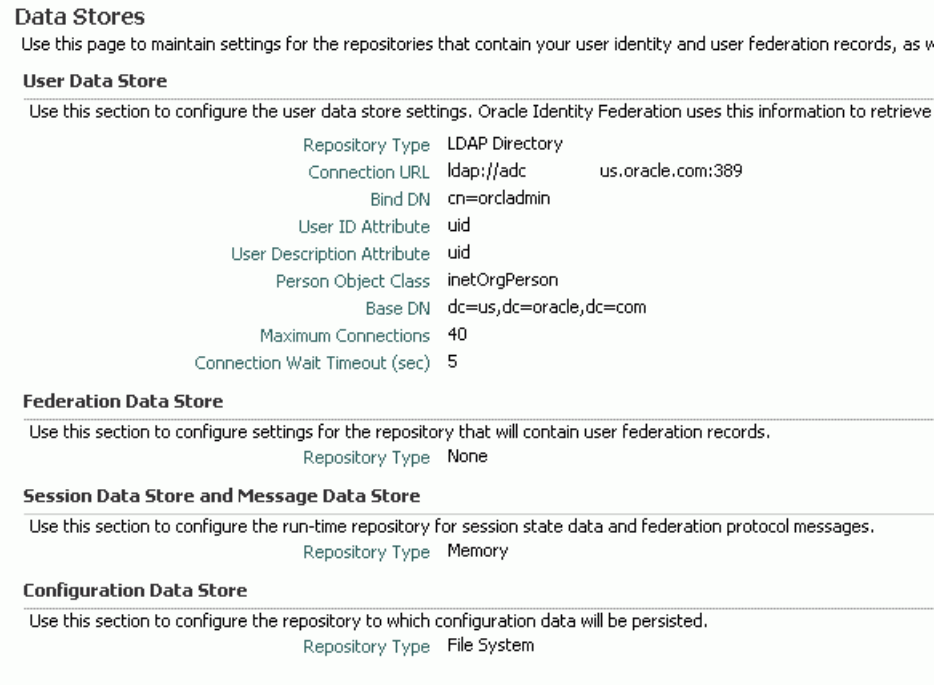
4. Check the **Load Metadata** box.
5. Click **Choose File**, and select the metadata file you generated for the IdP in Section 4.3.1, "Generated Provider Metadata".
6. Repeat the procedure to load metadata for the SP.

   Both providers appear in the list of trusted providers:



4.3.3 Configure Data Store

1. Locate the Oracle Identity Federation instance in Fusion Middleware Control.
2. Navigate to **Administration**, then **Data Stores**.
3. Specify the details of the user data store, as in this example:



4.3.4 Configure the Authentication Engine

In this task, the authentication engine is configured to point to a user data store, enabling Oracle Identity Federation to validate users against that store.

1. Locate the Oracle Identity Federation instance in Fusion Middleware Control.
2. Navigate to **Administration**, then **Authentication Engines**.
3. in the Default Authentication Engine drop down, select LDAP Directory.
4. Enter the user data store that was configured in the previous task, Section 4.3.3, "Configure Data Store".

4.3.5 Set the Default Identity Provider

This task sets the IdP that was created in an earlier task as the default IdP.

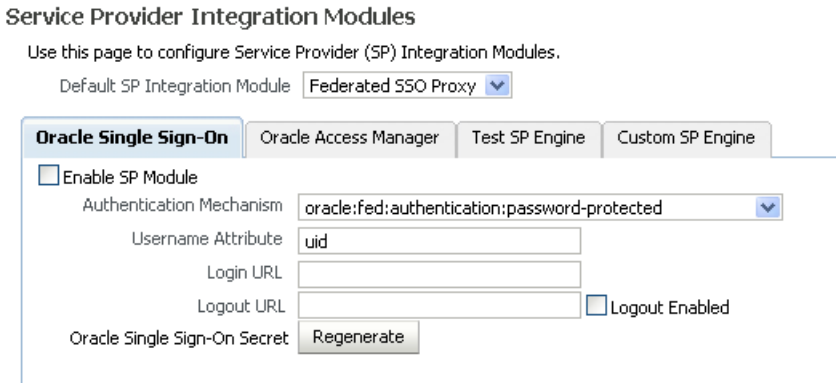
1. Locate the Oracle Identity Federation instance in Fusion Middleware Control.
2. Navigate to **Administration**, then **Service Provider**.
3. Check the **Enable Service Provider** box.
4. For Default SSO Identity Provider, specify the IdP set up in Section 4.3.2, "Register the Providers".
5. Click **Apply**.

4.3.6 Configure Oracle Identity Federation in SP Mode

Having generated the IdP/SP metadata and registered those modules, the final task of configuring Oracle Identity Federation for the integration is to provide the Oracle Access Manager server details, so that Oracle Identity Federation can send assertion tokens and direct session management to Oracle Access Manager.

The steps to achieve this are as follows:

1. Locate the Oracle Identity Federation instance in Fusion Middleware Control.
2. Navigate to **Administration**, then **Service Provider Integration Modules**.
3. Select the **Oracle Single Sign-On** tab.



4. Configure the page as follows:
   - In the **Default SP Integration Module** drop-down, select Oracle Single Sign On.
   - Check the **Enable SP Module** box.
   - Configure these URLs:

     ```
     Login URL  :  http://oam_host:oam_port/ngam/server/dap/cred_submit
     Logout URL :  http://oam_host:oam_port/ngam/server/logout
     ```

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

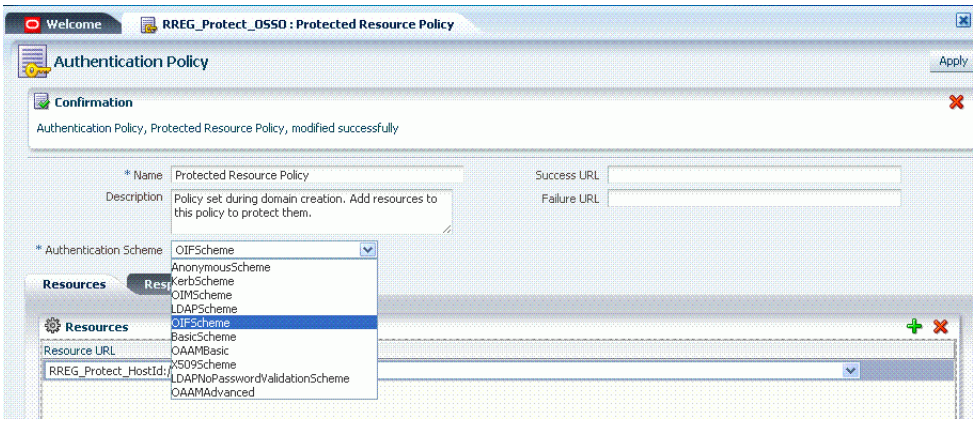
   This action generates a keystore file that contains the keys used to encrypt and decrypt the tokens that are exchanged between the Oracle Access Manager and Oracle Identity Federation servers.
6. Copy the keystore file to a location within the installation directory of Oracle Access Manager. Make a note of the location, since you will need to refer to it later.

4.4 Delegate Authentication to Oracle Identity Federation

As a result of performing the task in Section 4.2, "Register Oracle HTTP Server with Oracle Access Manager", clients seeking access to a protected resource are directed to Oracle Access Manager for authentication.

The final task in the integration procedure is to configure Oracle Access Manager to redirect the user to Oracle Identity Federation for authentication. The steps needed to achieve this are as follows:

1. Log in to the Oracle Access Manager Admin Console.
2. Select the **Policy Configuration** tab.
3. Protect the resource by selecting 'OIFScheme' in the **Authentication Scheme** drop-down.



4. Click **Apply**.
5. Copy the keystore file to a directory under the middleware home in which the Oracle Access Manager server is installed.
6. Use a WLST command to update the OIFDAP partner block in the `oam-config.xml` configuration file. The syntax is as follows:

   ```
   registerOIFDAPPartner(keystoreLocation=location of keystore file,
   logoutURL=logoutURL)
   ```

   where `logoutURL` is the Oracle Identity Federation logout URL to invoke when the Oracle Access Manager server logs out the user.

   For example:

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

Verification

To verify the action you took in Step 6 above, examine the `oam-config.xml` file to confirm that the properties in the OIFDAPPartner block were updated as mandated in Step 6.

If the configuration is correct, a logout initiated from Oracle Access Manager should cause logout in Oracle Identity Federation.

4.5 Test the Configuration

You can test that the integration is correctly configured by taking these steps:

1. Try accessing the protected resource.
2. When set up correctly, you should be redirected to an Oracle Identity Federation login page.
3. Enter valid credentials on the login page.

   Note: The user should exist in both the Oracle Identity Federation Data Store and in the Oracle Access Manager Embedded LDAP store.

4. Check that you are redirected to the protected page.

5. Verify that the following cookies are created:

```
OAM_ID
ORA_OSFS_SESSION
OHS Cookie
```

5

Integrating Oracle Access Manager and Oracle Adaptive Access Manager

This chapter describes how Oracle Access Manager can protect the Oracle Adaptive Access Manager console and leverage the authentication capabilities of Oracle Adaptive Access Manager. It contains these topics:

- Protecting the Oracle Adaptive Access Manager Console
- Authentication Features in Oracle Adaptive Access Manager
- Native Integration
- Advanced Integration
- Troubleshooting Tips

Note: Integration with Oracle Identity Manager provides additional features related to password collection. See Chapter 6, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager".

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

5.1 Protecting the Oracle Adaptive Access Manager Console

This section explains how to protect the Oracle Adaptive Access Manager administration console.

You can configure Oracle Access Manager to SSO-enable the Oracle Adaptive Access Manager administration console URL (/oaam_admin). In this setup, the OHS proxy for the URL is configured to use 11*g* WebGate.

With this configuration, users enter their credentials on the Oracle Access Manager login page, and are automatically logged into Oracle Adaptive Access Manager.

Topics in this section include:

- Prerequisites
- Integration Steps

5.1.1 Prerequisites

Ensure that the following prerequisites have been met before you perform the integration:

- All necessary components have been properly installed and configured:
  - Oracle Access Manager 11g has been installed and configured.
  - Oracle Adaptive Access Manager 11g has been installed and configured.
  - Oracle HTTP Server 11g has been installed and configured as a front-ending proxy web server for Oracle Adaptive Access Manager.
- Oracle Access Manager 11g agent (webgate) for Oracle HTTP Server 11g has been installed on the Oracle HTTP Server 11g instance

See the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* for additional information about these topics.

If the IdentityManagerAccessGate is not present, you need to create a new 10g WebGate profile for Oracle Adaptive Access Manager. Refer to Provisioning a 10g WebGate with OAM 11g in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager* for detailed instructions, and use the following information to configure the profile:

1. Use these values:
   - Name: OAAMAccessGate
   - Access Client Password: Set this to the same password configured for Oracle Adaptive Access Manager in the credential store framework. See Section 6.8.2, "Set Oracle Access Manager Credentials in Credential Store Framework"
   - Host Identifier: IDMDomain
   - Autocreate Policies: Uncheck this check box
2. Click **Apply**.
3. After changes are saved, update the primaryCookieDomain with your domain to be used.
4. Click **Apply**.

> **Note:** Make sure that you update the property `oaam.uio.oam.webgate_id` with the value `OAAMAccessGate` (used as the profile name above).

5.1.2 Integration Steps

Take these steps to configure Oracle Access Manager and Oracle Adaptive Access Manager to protect the Oracle Adaptive Access Manager administration console (oaam_admin URL):

1. Ensure that the required components are installed and configured as explained in Section 5.1.1, "Prerequisites".
2. Run the remote registration tool on the machine hosting Oracle HTTP Server 11g, to register Oracle Adaptive Access Manager as a partner application for the Oracle Access Manager agent.

See Also: Registering Partners (Agents and Applications) Remotely in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*

3. Log in to Oracle WebLogic Server Administration Console.

   For details, see Getting Started Using Oracle WebLogic Server Administration Console in the *Oracle Fusion Middleware Administrator's Guide*.

4. In Oracle WebLogic Server locate the Oracle Adaptive Access Manager provider page under myrealms, providers. Set up the Oracle Access Manager Identity Asserter and the OID Authentication provider. Oracle Adaptive Access Manager must be configured with these security providers.

   See Also: Configure Authentication and Identity Assertion providers in the Administration Console Online Help.

5. Restart all the Oracle WebLogic Servers including the administration server and Oracle Adaptive Access Manager managed servers.

6. In the Oracle Access Manager user identity store (typically, an LDAP store like OID), verify that there is a user belonging to the Oracle Adaptive Access Manager administrator group. If such a user is not present, take these steps:

   - Navigate to Security Realms and select your security realm.
   - Click the **Users and Groups** tab, then the **Users** sub-tab.
   - Use the **New** button to create a new user and assign the group named *OAAMRuleAdministratorGroup* to the new user.

7. In the Oracle HTTP Server environment, locate and open the `mod_wl_ohs.conf` configuration file.

8. Add an entry to the file using this format:

   ```
   MatchExpression /oaam_admin
   WebLogicHost=hostname.us.mycompany.com|WebLogicPort=WLS_port
   ```

   This entry configures Oracle HTTP Server to forward application requests to the Oracle WebLogic Server.

9. Restart Oracle HTTP Server.

10. Verify that the Oracle Adaptive Access Manager administration console is now protected by Oracle Access Manager and participates in single sign-on.

5.2 Authentication Features in Oracle Adaptive Access Manager

For strong authentication, Oracle Adaptive Access Manager provides a comprehensive set of challenge question functionality, which includes challenging the user before and after authentication as required with a series of questions.

In addition to challenge questions, Oracle Adaptive Access Manager also provides images and various input devices.

Oracle Adaptive Access Manager also has a capability to ask questions one after another, revealing the questions only if correct answers are provided.

Your site can leverage Oracle Adaptive Access Manager features through one of these options:

- Native Integration
- Advanced Integration

5.3 Native Integration

In the native integration, Oracle Access Manager leverages Oracle Adaptive Access Manager features to provide pre- and post-authentication flow for logins, without requiring an Oracle Adaptive Access Manager server.

With native integration, the Oracle Adaptive Access Manager libraries and configuration interface for different flows (challenge, registration, and so on) are bundled with the Oracle Access Manager server. Although Oracle Adaptive Access Manager determines the strong authentication flows, these are rendered by the Oracle Access Manager server. Oracle Access Manager invokes the Oracle Adaptive Access Manager APIs to apply pre- and post-authentication rules, and based on the results, displays the next set of pages and performs necessary processing. Control is never transferred out of the Oracle Access Manager server.

For this type of integration, the Oracle Adaptive Access Manager database must be operational.

KBA is the only challenge mechanism available in this 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
- Authentication Scheme
- Prerequisites
- Native Integration Steps
- How to Implement Case-Insensitive Logins

5.3.1 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. Oracle Access Manager calls the Oracle Adaptive Access Manager APIs again, to run post-authentication rules. 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.

5.3.2 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*.

5.3.3 Prerequisites

The prerequisites are as follows:

- Install the Oracle Access Manager server.
- Install the Oracle Adaptive Access Manager server and database.
- For testing, remote-register two agents, each protecting a resource.
- 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*.

5.3.4 Native Integration Steps

Take these steps to implement the Oracle Access Manager-Oracle Adaptive Access Manager integration:

1. Locate the `oam-config.xml` file.
2. Enable the `OAAMEnabled` property in the oam-config.xml file by setting it to "true".

   A portion of the file with this property enabled will look like this:

```
<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>
```

3. Create a schema on the Oracle Adaptive Access Manager database with a descriptive schema name; for example, "NATIVE_OAAM".
4. Access the Oracle WebLogic Server console.
5. 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.

6. To the schema you created in Step 3, provide the connection details for the Oracle Adaptive Access Manager database.
7. Associate Administration Server and oam_server1 as targets with the datasource.
8. Access the Oracle Adaptive Access Manager administration console.
9. Import the policies file containing the specified scheme into the Oracle Adaptive Access Manager database using the Oracle Adaptive Access Manager Administration console.
10. Associate the protected resource with the OAAMBasic scheme.
11. Access the protected resource to verify the configuration.

5.3.5 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 username 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 username userXY.

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

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

5.4 Advanced Integration

With advanced integration, Oracle Adaptive Access Manager provides the strong authentication flow for Oracle Access Manager logins, including:

- virtual authenticators
- fraud rules
- KBA and OTP functionality

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

5.4.1 Processing Flow for Advanced Integration

For details of the processing flow for interaction between Oracle Access Manager and Oracle Adaptive Access Manager, see Section 2.8.2.2, "Component Interactions".

5.4.2 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 6, "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 Chapter 6, "Integrating Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager", omitting Oracle Identity Manager-related configuration of the Oracle Identity Manager server, and omitting the steps in Section 6.10, "Configure Oracle Identity Manager Properties for the Integration".

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

`http://host:<oaam-server-port>/oaam_server/oamLogout.jsp`

5.5 Troubleshooting Tips

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

- Using Non-ASCII Credentials

5.5.1 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.
```

Take 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

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 for secure password collection:

6.1 Introduction

In 11*g* 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
- 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

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 protection through personalized virtual authenticators
- KBA challenge questions for secondary login authentication based on risk
- OTP challenge for secondary login authentication based on risk
- Registration flows to support password protection and KBA and OTP challenge functionality
- User preferences 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 fraud rules before and after authentication
- Navigating the user through Oracle Adaptive Access Manager flows based on the outcome of fraud rules

Oracle Identity Manager

Oracle Identity Manager is responsible for:

- Provisioning users (add/modify, delete users)
- Managing passwords (reset/change password)

Oracle Access Manager

Oracle Access Manager is responsible for:

- Authenticating and authorizing users
- Providing statuses such as Reset Password, Password Expired, User Locked, and others

6.2 Process Flow

In this deployment, Oracle Access Manager redirects users to Oracle Adaptive Access Manager when a trigger condition for password management is in effect. The "trigger condition" is the authentication scheme used in Oracle Access Manager.

Oracle Adaptive Access Manager interacts with the user based on lifecycle policies retrieved from Oracle Access Manager, and when the condition is resolved, notifies Oracle Access Manager so that the user is redirected to the protected resource. In this integration, Oracle Identity Manager serves to provide password policy enforcement.

For a detailed description of the processing flow see Section 2.8, "Integrating Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive Access Manager"

6.3 Prerequisites

The following needs to be in place for the integration:

- All necessary components have been properly installed and configured:
  - Oracle Internet Directory 11g installed

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

  - Oracle Virtual Directory 11g installed

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

  - Repository Creation Utility 11g installed

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

  - Oracle WebLogic Servers installed

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

  - SOA suite installed and patched to at least PS2

    For information on installing the 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 11*g* agent (WebGate) for Oracle HTTP Server 11*g* has been 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*.

- At installation, Oracle Access Manager is configured with the database policy store. The Oracle Access Manager-Oracle Adaptive Access Manager wiring requires the database policy store.

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.

6.4 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
- 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 Oracle Access Manager Policy Authentication Scheme
- Restart the Servers

6.5 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 servers with all three in the same domain.

Perform post-configuration for Oracle Access Manager and Oracle Adaptive Access Manager with the out-of-the-box configuration.

Ensure that the out-of-the-box policies and KBA questions are configured; this is important for Oracle Adaptive Access Manager authentication to work. For details on these default policies and questions, see:

- Importing Challenge Questions in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*
- Importing Base Policies in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*

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

6.6 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, Oracle Identity Manager.

For information on integrating Oracle Access Manager and Oracle Identity Manager, refer to Integration Between OIM and OAM in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

6.7 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, Oracle Identity Manager.

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

For information about setting up Oracle Identity Manager for LDAP synchronization, refer to OIM with LDAP Sync in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

6.8 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 to deliver password management and challenge-related functionality to Oracle Access Manager-protected applications.

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**.

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 - Oracle Identity Manager integration (see Section 6.6, "Integrate Oracle Access Manager and Oracle Identity Manager").

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

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

6.8.1 Set Oracle Adaptive Access Manager Properties for Oracle Access Manager

Note: Before doing this procedure, you must take into account whether the OAAM 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 console, then the user must be created in the WebLogic Administration Console.

  (*Note* : You can disable OAAM 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:

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 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 6–1 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.oracle.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 *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".

6.8.2 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. Go to the Oracle Fusion Middleware Enterprise Manager Console at `http://WebLogic Server Host:Administration 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, 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**.

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

6.9 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

6.9.1 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 Oracle Adaptive Access Manager Admin Console at `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 6–2 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.oracle.com:14000`
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.
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*.

6.9.2 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 Server host>:<Administration 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 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 window make sure **Select Map** is **oaam**.
8. Provide the following properties and click **OK**.

Name	Value
Map Name	oaam
Key Name	oim.credentials
Key Type	Password
UserName	Username of Oracle Identity Manager Administrator
Password	Password of Oracle Identity Manager Administrator

6.10 Configure Oracle Identity Manager Properties for the Integration

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

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

1. Log in to 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 6–3 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.ForgotPasswordURL	URL for forgot password page in Oracle Adaptive Access Manager (`http://`*OAAM Server Managed Server Host:OAAM Server Managed Server Port*`/oaam_server/oimForgotPassword.jsp`)
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`)

6.11 Configure Oracle Access Manager Policy Authentication Scheme

Change your protected web application's Oracle Access Manager policy to point 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 using a URL of the form `http://`*hostname*:*port*`/oamconsole`.

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

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 for editing the authentication policy named `Protected HigherLevel Policy`, and assign to it the `OAAMAdvanced` authentication scheme.

5. Test the Oracle Adaptive Access Manager URL in a separate browser session by navigating to:

   `http://`*OAAM Server Managed Server Host: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. Set the Oracle Adaptive Access Manager URL by navigating to the **OAAMAdvanced** authentication scheme and 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.

6.12 Restart the Servers

Once integration between Oracle Access Manager and Oracle Adaptive Access Manager is complete, restart the managed servers:

1. Start the managed server hosting the Oracle Access Manager server.
2. Restart the Oracle Adaptive Access Manager managed servers (OAAM Admin and OAAM server).

6.13 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.

6.13.1 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*.

6.13.2 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.oracle.com`.

7

Configuring Oracle Access Manager to use Windows Native Authentication

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

7.1 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 7.3, "Performing Prerequisite Tasks"

7.2 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.

7.3 Performing Prerequisite Tasks

The integration tasks are as follows:

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

7.3.1 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.oracle.com
admin_server = holmium.us.oracle.com
default_domain = HOLMIUM.NGAM.COM
}

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

7.3.2 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.mycorp.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.mycorp.com then the principal name is HTTP/mynode47.us.mycorp.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.

7.3.3 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.mycorp.com@HOLMIUM.NGAM.COM -k -t
   /scratch/kerberos/keytab.service
   ```

   where:

   - -V indicates verbose mode
   - principal name is HTTP/mynode47.us.mycorp.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".

7.4 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

7.4.1 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>.oracle.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".

7.4.2 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".

7.4.3 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.

7.4.4 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.mycorp.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>
```

7.5 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`

7.6 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.

7.7 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

W