Oracle® Fusion Middleware

Integration Guide for Oracle Identity Management Suite

12c (12.2.1.4.0)
E95932-14
April 2023

ORACLE

Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite, 12c (12.2.1.4.0)

E95932-14

Primary Author: Oracle Corporation

Contents

List of Figures

List of Tables

Preface

This guide describes how you can integrate certain components in the Oracle Identity Management suite to provide a broad range of solutions for application environment including: integration with LDAP repositories, identity and access management, advanced login and password security, and identity federation.

Audience

This document is intended for administrators who wish to integrate Oracle Identity Management components using a simple topology without high availability features.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents in the documentation set:

- Oracle Access Management in *Release Notes for Oracle Identity Management*
- Oracle Identity Governance in *Release Notes for Oracle Identity Management*
- Introduction to Oracle Access Management in *Administering Oracle Access Management*
- Product Overview for Oracle Identity Governance in *Administering Oracle Identity Governance*

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.

Convention	Meaning
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New

This preface provides a summary of new features and updates to Oracle Identity Management suite integration.

New and Changed Features for 12*c* (12.2.1.4.0)

Configuring Role UDF is supported for the following integrations:

- OIM-OAM integration setup created using Integrating OIG with OAM and LDAP Connectors.
- LDAP Connector Sync support for non OAM installations using `Doc ID 2833544.1` at https://support.oracle.com.

For more information, see Configuring Role UDFs.

This release also addresses bug fixes.

New and Changed Features for 12*c* (12.2.1.3.0)

The *Integration Guide for Oracle Identity Management Suite* contains these new features:

- Execute the new automated script, `OIGOAMIntegration.sh` to accomplish OIG-OAM integration in a single step. The script utilizes user-supplied values from property files to perform various configurations. See One-step Procedure for OIG-OAM Integration Using Automated Script.
- Alternatively, execute individual configuration steps sequentially to accomplish the integration incrementally. This is done by running the new automated script, `OIGOAMIntegration.sh` several times, each time with a different parameter to specify which operation to be performed. See Step-by-step Procedure for OIG-OAM Integration Using Automated Script.

The following additional updates have been made to this document:

- Bug fixes and other corrections have been applied.
- Links have been added to key integration procedures that reside in other documents.

Part I

Oracle Identity Management Integration Topology

This part introduces the supported integration topologies, and describes the tools used during integration.

See:

Introduction to Oracle Identity and Access Management Suite Components Integration

1

Introduction to Oracle Identity and Access Management Suite Components Integration

This chapter explains integration concepts for the Oracle Identity and Access Management suite.
The chapter contains these topics:

- Prerequisites to Integrating Oracle Identity Management Suite Components
- Understanding Oracle Identity Management Integration Topologies
- Overview of Oracle Identity Management Components Used in the Integration
- Oracle Identity Management Integration Quick Links
- About Password Management Scenarios
- System Requirements and Certification
- Using My Oracle Support for Additional Troubleshooting Information

1.1 Prerequisites to Integrating Oracle Identity Management Suite Components

Before using these procedures to integrate Identity Management components, you must install and deploy the components.

These prerequisites are explained in the following sections:

- Understanding the Installation Roadmap
- Understanding Deployment Topologies
- Understanding the Identity Store
- Understanding Integration Between LDAP Identity Store and Oracle Identity Governance
- Common Environment Variables
- Operating System

For details about installing Identity Management components, see About the Oracle Identity and Access Management Installation in *Installing and Configuring Oracle Identity and Access Management*.

1.1.1 Understanding the Installation Roadmap

You will take (or may already have taken) one of these paths in your IdM deployment:

- Installation, followed by component integration, and ending with scale-out (HA)
- Installation, followed by scale-out, and ending with integration

With scale-out, you may already have performed some of the integration procedures described here; notes in the relevant sections can help you determine whether a procedure is needed.

Using the Standard Installation Topology as a Starting Point in the *Installing and Configuring Oracle Identity and Access Management* contains background on the deployment procedure and describes the installation topology, prerequisites, and the installation and configuration workflow.

Oracle Identity Governance High Availability Concepts and Oracle Access Manager High Availability Concepts chapters in the *Installing and Configuring Oracle Identity and Access Management* explains the high availability solutions in Oracle Fusion Middleware, as well as the topologies and architecture of the various high availability options.

For informaiton about integrating Oracle Access Manager and LDAP, see Integrating Oracle Access Manager and LDAP.

For information about integrating Oracle Access Manager and Oracle Identiy Governance, see Integrating Oracle Identity Governance with Oracle Access Manager and LDAP Connectors.

1.1.2 Understanding Deployment Topologies

Before starting this integration, you must also understand the identity management topology and the environment in which the components will work together.

To learn more about the topology supported in this document, see Understanding Oracle Identity Management Integration Topologies.

1.1.3 Understanding the Identity Store

Oracle Identity Governance provides the ability to integrate an LDAP-based identity store into Oracle Identity Governance architecture. You can connect and manage an LDAP-based identity store directly from Oracle Identity Governance. Using this feature, you can use advanced user management capabilities of Oracle Identity Governance, including request-based creation and management of identities, to manage the identities within the corporate identity store.

In this deployment architecture, user identity information is stored in Oracle Identity Governance database to support the relational functionality necessary for Oracle Identity Governance to function, as well as in the LDAP store. All data is kept in sync transparently without the need for provisioning actions and setting up policies and rules. Identity operations started within Oracle Identity Governance, such as user creation or modification, are run on both the stores in a manner that maintains transactional integrity. In addition, any changes in the LDAP store made outside of Oracle Identity Governance are pulled into Oracle Identity Governance and made available as a part of the identity context.

1.1.4 Understanding Integration Between LDAP Identity Store and Oracle Identity Governance

Oracle Identity Governance users and roles are stored in the Oracle Identity Governance database. However, when a user, role, or role membership change takes

place in Oracle Identity Governance, this information is propagated to the LDAP identity store. If a user, role, or role membership change takes place in LDAP directly, then these changes are synchronized into Oracle Identity Governance. The synchronization involves:

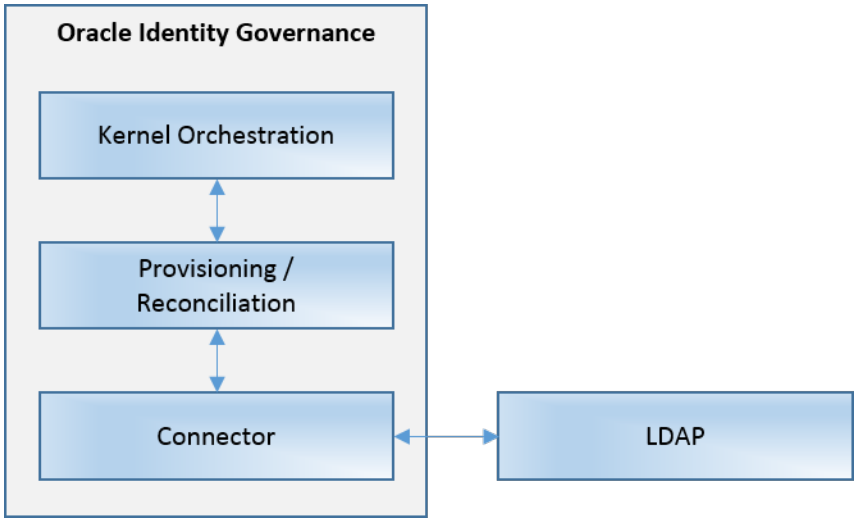
- Changes made in Oracle Identity Governance: User creation, modification, deletion, changes in enabled/disabled state and locked/unlocked states, and password changes are synchronized to LDAP.
- Role creation, modification, and deletion actions update the LDAP groups, including membership changes.
- Initial load of users, roles, and role memberships are synchronized.
- Direct changes to user profile in LDAP are reconciled to Oracle Identity Governance. However, a change to a user password made in LDAP is not reconciled to Oracle Identity Governance.
- Direct changes to roles and role memberships in LDAP are reconciled to Oracle Identity Governance.

When changes are made in the user and role data, the actual operation is performed with the help of the kernel handlers. These handlers go through an orchestration lifecycle of various stages, such as validation, preprocessing, action, and postprocessing.

Synchronization between Oracle Identity Governance and LDAP is performed by an LDAP connector library.

Figure 1-1 shows the communication between Oracle Identity Governance and LDAP.

Figure 1-1 Oracle Identity Governance and LDAP



1.1.4.1 Configuring the Integration with LDAP

Configuring the integration between Oracle Identity Governance and LDAP is performed after installing Oracle Identity Governance. See Scheduled Jobs for OIG-OAM Integration.

1.1.5 Common Environment Variables

Shorthand notations are used to refer to common environment variables.

For example, the Oracle Middleware Home directory is often referred to as `MW_HOME`.

1.1.6 Operating System

Currently, only Unix operating system is supported when integrating.

For details, see the note `Is Oracle Access Manager(OAM) Integrated With Oracle Identity Governance(OIG) Supported On The Windows Operating System(OS) (Doc ID 2780529.1)` at https://support.oracle.com .

1.2 Understanding Oracle Identity Management Integration Topologies

Oracle Identity Management consists of a number of products, which can be used either individually or collectively.

Two basic types of topology are available in Oracle Identity Management:

- Basic integration topology

  This topology supports integration between suite components, in an environment where each component runs on a separate node.

- Enterprise integration topology

  This topology supports integration between suite components in an enterprise environment. Each component may run on multiple nodes.

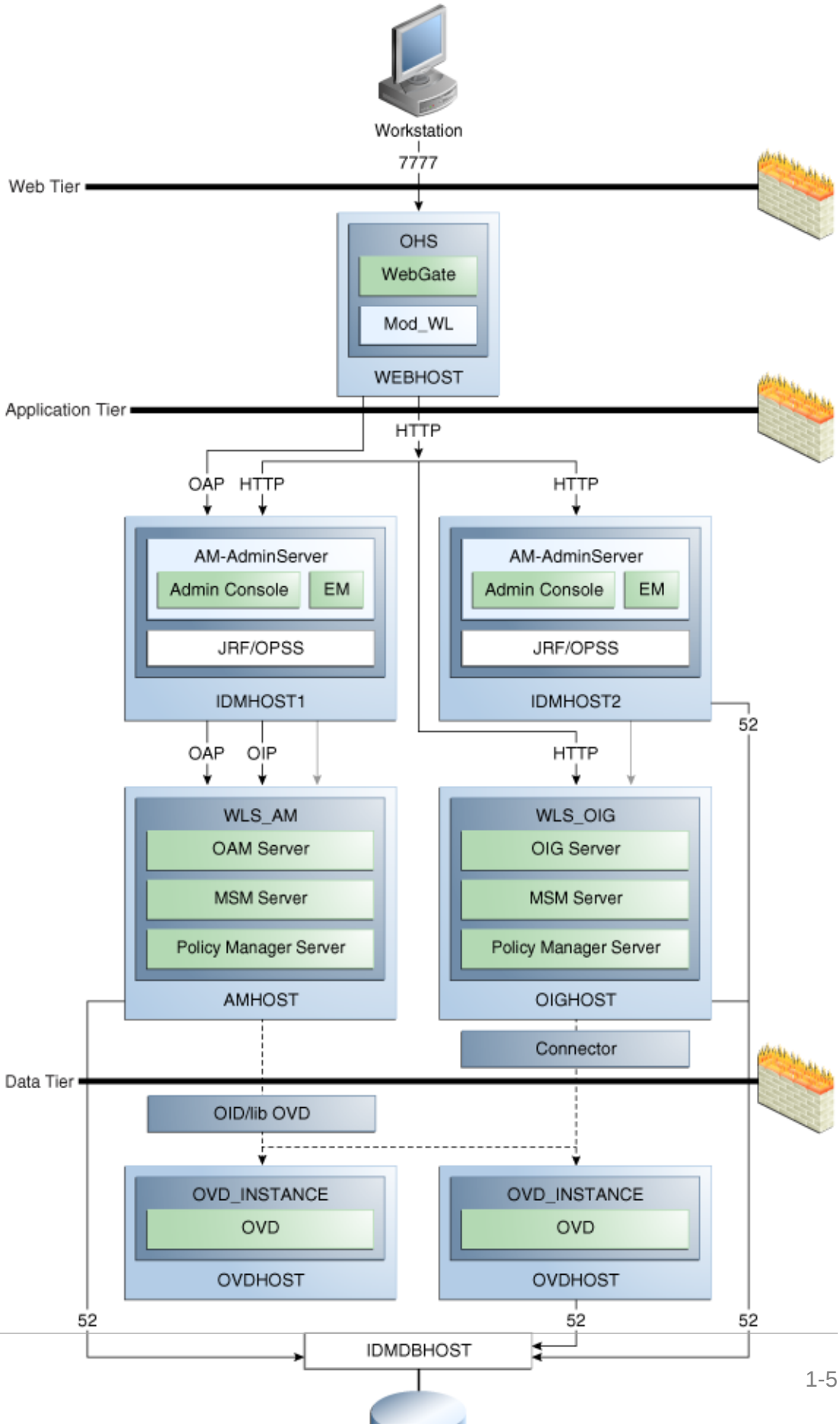
This book is dedicated to the first type, single-node integration topology. Use the procedures described in this book when deploying Oracle Identity Management in an environment where each component runs on its own node. You can also use the procedures to understand integration tools and techniques, and to understand the effects and benefits of integrating specific identity management components.

1.2.1 About the Basic Integration Topology

Basic integration topology is where the IdM components Access Manager and Oracle Identity Governance are configured on separate Oracle WebLogic domains.

> **See Also:**
>
> Table 1-1 for definitions of acronyms used in this section.

Figure 1-2 Basic Integration Topology with Multiple Administration Servers



The above diagram shows a basic integration topology where the IdM components Access Manager and Oracle Identity Governance are configured on separate Oracle WebLogic domains:

Note that:

- All IdM components, including Access Manager server (`AMHOST`), the Oracle Identity Governance server (`OIGHOST`), and Oracle Internet Directory (OID) are configured in separate WebLogic domains, and each is administered by its own administration server.

  Besides enhancing management of each component, this topology ensures you have flexibility when applying patches and upgrades. Patches for each component can be applied independently, with no version dependency on other components.
- For simplicity, some of the OMSS topology is omitted; for example the MSAS server which resides in the DMZ is not shown in the diagram.
- The BIP server and SOA Suite reside on the OIG domain; they are not shown in the diagram.
- The figure shows some representative ports only.

The SOA Suite used by OIG must be installed in the same domain as OIG. However, if you use SOA Suite for other purposes, you should consider setting up a separate install of SOA Suite for running your own services, composites, and other SOA features for that purpose.

In the single-domain architecture, Oracle Access Management Access Manager, Oracle Identity Governance, and Oracle Mobile Security Access Server are configured on the same WebLogic domain. While possible, such a topology is not practical in the current context for the reasons cited above, and is not recommended for IdM integration.

> **See Also:**
>
> Overview of Oracle Identity Management Components Used in the Integration for an introduction to each IdM component.

1.2.1.1 About the Three Tier Architecture

This architecture can be viewed as consisting of three layers or zones:

- The Web Tier consists of the HTTP server and handles incoming Web traffic.
- The Application Tier contains identity management applications for managing identities and access, including Oracle Identity Management and Oracle Access Manager.
- The Data Tier, here considered to include the directory servers, hosts LDAPs and database.

1.2.1.2 Understanding the Web Tier

The web tier is in the DMZ Public Zone. The HTTP servers are deployed in the web tier.Most Identity Management components can function without the web tier. However,

the web tier is required to support enterprise level single sign-on using products such as Access Manager.

The web tier is structured as follows in the single-node topology:

- `WEBHOST` has Oracle HTTP Server, WebGate (an Access Manager component), and the mod_wl_ohs plug-in module installed. The mod_wl_ohs plug-in module enables requests to be proxied from Oracle HTTP Server to a WebLogic Server running in the application tier.WebGate, an Access Manager component in Oracle HTTP Server, uses Oracle Access Protocol (OAP) to communicate with Access Manager running on `OAMHOST`. WebGate and Access Manager are used to perform operations such as user authentication.

1.2.1.3 Understanding the Application Tier

The application tier is the tier where Java EE applications are deployed. Products such as Oracle Identity Governance, Oracle Mobile Security Suite, Oracle Access Management Identity Federation, and Oracle Enterprise Manager Fusion Middleware Control are among key Java EE components deployed in this tier.

The Identity Management applications in the application tier interact with the directory tier as follows:

- They leverage the directory tier for enterprise identity information.
- They leverage the directory tier (and sometimes the database in the data tier) for application metadata.
- Fusion Middleware Control Console provides administrative functions to the components in the application and directory tiers.
- Oracle WebLogic Server has built-in web server support. If enabled, the HTTP listener exists in the application tier as well.

1.2.1.4 Understanding the Data Tier

The data tier is the deployment layer where all the LDAP services reside. This tier includes products such as Oracle Internet Directory (`OIDHOST`), Oracle Unified Directory, and Oracle Database (`IDMDBHOST`).

The data tier stores two types of information:

- Identity Information: Information about users and groups resides in the identity store.
- Oracle Platform Security Services (OPSS): Information about security policies and about configuration resides in the policy store.

Policy information resides in a centralized policy store that is located within a database. You may store identity information in Oracle Internet Directory or in another directory.

> **Note:**
>
> Oracle Access Manager uses Oracle Virtual Directory server or libOVD to access third-party directories.

1.2.2 About the Enterprise Integration Topology

Unlike single-node topologies, an enterprise integration topology takes into account such features as high availability, failover, and firewalls, and is beyond the scope of this document.

1.2.3 Integration Terminology

Definitions of terms that define the Oracle Fusion Middleware architecture.

Table 1-1 shows key terms and acronyms that are used to describe the architecture and topology of an Oracle Fusion Middleware environment:

Table 1-1 Oracle Fusion Middleware Integration Terminology

Term	Definition
IdM Configuration Tool	A command-line tool to verify the status of identity management components and to perform certain integration tasks.
Oracle Access Protocol (OAP)	A secure channel for communication between Webgates and Access Manager servers during authorization.
Oracle Fusion Middleware home	A **Middleware home** consists of the Oracle WebLogic Server home, and, optionally, one or more Oracle homes. A Middleware home can reside on a local file system or on a remote shared disk that is accessible through NFS.
Oracle HTTP Server (OHS)	Web server component for Oracle Fusion Middleware that provides a listener for Oracle WebLogic Server.
WebLogic Server home	A **WebLogic Server home** contains installed files necessary to host a WebLogic Server. The WebLogic Server home directory is a peer of other Oracle home directories underneath the Middleware home directory.
Oracle home	An **Oracle home** contains installed files necessary to host a specific product. For example, the Oracle Identity Management Oracle home contains a directory that contains binary and library files for Oracle Identity Management. An Oracle home resides within the directory structure of the Middleware home. Each Oracle home can be associated with multiple Oracle instances or Oracle WebLogic Server domains.
Oracle instance	An **Oracle instance** contains one or more system components, such as Oracle Web Cache, Oracle HTTP Server, or Oracle Internet Directory. The system components in an Oracle instance must reside on the same machine. An Oracle instance directory contains files that can be updated, such as configuration files, log files, and temporary files. An Oracle instance is a peer of an Oracle WebLogic Server domain. Both contain specific configurations outside of their Oracle homes. The directory structure of an Oracle instance is separate from the directory structure of the Oracle home. It can reside anywhere; it need not be within the Middleware home directory.

Table 1-1 (Cont.) Oracle Fusion Middleware Integration Terminology

Term	Definition
Oracle WebLogic Server domain	A **WebLogic Server domain** is a logically related group of Java components. A WebLogic Server domain includes a special WebLogic Server instance called the Administration Server, which is the central point from which you configure and manage all resources in the domain. Usually, you configure a domain to include additional WebLogic Server instances called Managed Servers. You deploy Java components, such as Web applications, EJBs, and Web services, and other resources to the Managed Servers and use the Administration Server for configuration and management purposes only. Managed Servers in a WebLogic Server domain can be grouped together into a cluster. An Oracle WebLogic Server domain is a peer of an Oracle instance. Both contain specific configurations outside of their Oracle homes. The directory structure of an WebLogic Server domain is separate from the directory structure of the WebLogic Server home. It can reside anywhere; it need not be within the Middleware home directory.
system component	A **system component** is a manageable process that is not WebLogic Server. For example: Oracle HTTP Server, WebCache, and Oracle Internet Directory. Includes the JSE component.
Java component	A **Java component** is a peer of a system component, but is managed by the application server container. Generally refers to a collection of applications and resources, with generally a 1:1 relationship with a domain extension template. For example: SOA and WebCenter Spaces.
Oracle Fusion Middleware farm	Oracle Enterprise Manager Fusion Middleware Control is a Web browser-based, graphical user interface that you can use to monitor and administer an Oracle Fusion Middleware farm. An **Oracle Fusion Middleware farm** is a collection of components managed by Fusion Middleware Control. It can contain WebLogic Server domains, one or more Managed Servers and the Oracle Fusion Middleware system components that are installed, configured, and running in the domain.
Oracle Identity Management	The suite of identity and access management components in Oracle Fusion Middleware. See Overview of Oracle Identity Management Components Used in the Integration for details.
WebLogic Administration Server	The Administration Server is the central point from which you configure and manage all resources in the WebLogic domain.
WebLogic Managed Server	The Managed Server is an additional WebLogic Server instance to host business applications, application components, Web services, and their associated resources. Multiple managed servers can operate within the domain. Certain Managed Servers in the domain are created specifically to host Oracle Fusion Middleware components.

1.3 Overview of Oracle Identity Management Components Used in the Integration

This section provides a brief overview of Oracle Identity Management components whose integrations are described in this guide, and explains the benefits of integration.

Topics include:

- Oracle Unified Directory
- Oracle Internet Directory
- Oracle Access Management Access Manager
- Oracle Identity Governance
- Oracle Access Management Identity Federation

1.3.1 Oracle Unified Directory

Oracle Unified Directory is a comprehensive next generation directory service. It is designed to address large deployments and to provide high performance in a demanding environment.

The Oracle Unified Directory server is an LDAPv3-compliant directory server written entirely in Java. The directory server provides full LDAPv3 compliance, high performance and space effective data storage, and ease of configuration and administration.

Several procedures in this book feature Oracle Unified Directory as the repository for the identity store.

1.3.2 Oracle Internet Directory

Oracle Internet Directory is a general purpose directory service that enables fast retrieval and centralized management of information about dispersed users and network resources. It combines Lightweight Directory Access Protocol (LDAP) Version 3 with the high performance, scalability, robustness, and availability of an Oracle Database.

Oracle Internet Directory can serve as the repository for the identity store, which contains user identities leveraged by identity management components and other applications.

1.3.3 Oracle Access Management Access Manager

Oracle Access Management Access Manager provides a full range of Web perimeter security functions that include Web single sign-on; authentication and authorization; policy administration; auditing, and more. All existing access technologies in the Oracle Identity Management stack converge in Access Manager.

For details about integration with Access Manager, see:

- Integrating with Identity Federation

1.3.3.1 A Note About IDMDomain Agents and Webgates

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

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

1.3.4 Oracle Identity Governance

Oracle Identity Management is a powerful and flexible enterprise identity management system that automatically manages users' access privileges within enterprise IT resources. Oracle Identity Governance 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.

1.3.5 Oracle Access Management Identity Federation

To enhance support for federated authentication in cloud, web services, and B2B transactions, a SAML-based federation service is being introduced in a single access management server in 11*g* Release 2 (11.1.2). Oracle Access Management Identity Federation is an enterprise-level, carrier-grade service for secure identity information exchange between partners. Identity Federation protects existing IT investments by integrating with a wide variety of data stores, user directories, authentication providers and applications.

In this initial release Identity Federation is limited to Service Provider mode. Identity Provider mode still requires an Oracle Identity Federation 11gR1 installation.

For details about using the Identity Federation service with Access Manager, see Integrating with Identity Federation.

1.4 Oracle Identity Management Integration Quick Links

Links to integration procedures.

Table 1-2 provides links to the integration procedures described here.

Table 1-2 Links to Integration Procedures in This Guide

Components to Integrate	Link
Access Manager and LDAP Directory	Integrating Oracle Access Manager and LDAP
Access Manager and Oracle Identity Governance	Integrating Oracle Identity Governance with Oracle Access Manager and LDAP Connectors
Access Manager and Identity Federation	Integrating with Identity Federation
Multi-Directory identity store	Configuring an Identity Store with Multiple Directories

Table 1-3 lists key integration procedures that appear in other Oracle Identity Management documents:

Table 1-3 Links to Integration Procedures in Other Guides

Components to Integrate	Link
OIG and Oracle Identity Analytics (OIA)	Integrating with Identity Analytics in *Administering Oracle Identity Governance*

1.5 About Password Management Scenarios

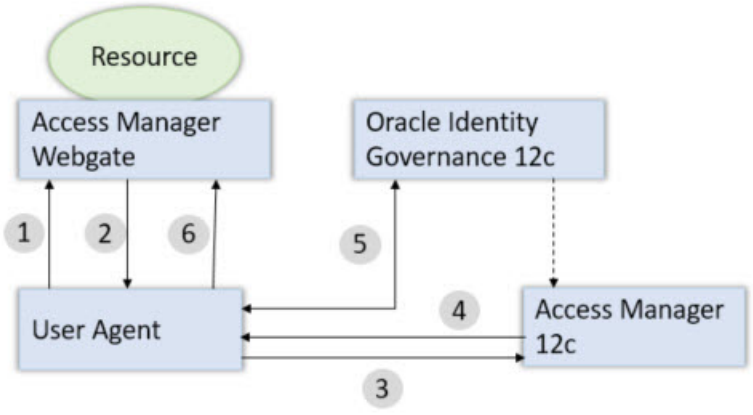
Common management scenarios supported by these deployment modes include:

- About Access Manager Integrated with Oracle Identity Governance
- About Self-Registration
- About Password Change
- About Forgot Password
- About Account Lock and Unlock
- About Challenge Setup

1.5.1 About Access Manager Integrated with Oracle Identity Governance

#unique_55/unique_55_Connect_42_CFHIDBEI shows how password management is achieved when Access Manager and Oracle Identity Governance are integrated.

Figure 1-3 Integrating Access Manager and Oracle Identity Governance for Password Management



The flow of interactions between the components is as follows:

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

1.5.2 About Self-Registration

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

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

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 self-registration page. The options are:
>
> - Self-registration using the default self-registration page or a customized version of the 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.

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

1.5.3 About Password Change

The Change Password flow enables users to change their password.

In the Change Password flow with Access Manager and Oracle Identity Governance, the user successfully logs into 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, Access Manager detects if the triggering condition is in effect and redirects the user to the Oracle Identity Governance **Change Password** URL. Oracle Identity Governance facilitates the user password change or challenge set-up and resets the triggering condition.

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

This situation is triggered in the following cases:

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

This flow describes the situation where a user logs in to an 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 Access Manager.
2. Oracle Access Management WebGate (SSO Agent) intercepts the request and redirects the user to the Access Manager Login Page.

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

1.5.4 About Forgot Password

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

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

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

On completion, Oracle Identity Management 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 Access Manager.
2. The Oracle Access Management WebGate (SSO Agent) intercepts the request and redirects the user to the Access Manager Login Page.
3. The user clicks on the **Forgot Password** link on the Access Manager Login page, which sends the user to the Oracle Identity Governance **Forgot Password** URL.
4. Oracle Identity Governance interacts with the user to enable the user to reset the password. On completion, Oracle Identity Governance performs a user auto-login.
5. Oracle Identity Governance redirects the user to the application URL to which access was attempted in step 1.

1.5.5 About Account Lock and Unlock

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

After the user account is locked, Access Manager displays the Help Desk contact information and Forgot Password link, or similar for any login attempt made. The information provided

about the account unlocking process will need to be customized to reflect the process that is followed by your organization.

The following describes the account locking/unlocking flow:

1. Using a browser, a user tries to access an application URL that is protected by Access Manager.
2. Oracle Access Management WebGate (SSO Agent) intercepts the request and redirects the user to the Access Manager login page.
3. The user submits credentials that fail Access Manager validation. Access Manager renders the login page and asks the user to resubmit his or her credentials.
4. The user's unsuccessful login attempts exceed the limit specified by the policy. Access Manager locks the user account and redirects the user to the Access Manager Account Lockout URL. The resulting page displays the Help Desk contact information and Forgot Password link.
5. If the user contacts the Help Desk over the telephone and asks an administrator to unlock the account, then:
    a. The Help Desk unlocks the account using the Oracle Identity Governance administration console.
    b. Oracle Identity Governance notifies Access Manager of the account unlock event.
    c. The user attempts to access an application URL and this event triggers the normal Oracle Access Management single sign-on flow.
6. If the user uses the **Forgot Password** link, the user is sent to the Oracle Identity Governance Forgot Password URL, then:
    a. Oracle Identity Governance interacts with the user to enable the user to reset the password. On completion, Oracle Identity Governance performs a user auto-login.
    b. Oracle Identity Governance redirects the user to the application URL.

> **Note:**
>
> The user would be able to self-unlock the account by going through the Oracle Identity Governance Forgot Password flow, only once the user status is locked in Oracle Identity Governance. The user locked status is synchronized from the LDAP provider to Oracle Identity Governance only when the "SSO User Incremental Reconciliation" or "SSO User Full Reconciliation" scheduled job is run.

1.5.6 About Challenge Setup

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

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

Access Manager detects and redirects on password trigger conditions:

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

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

1.6 System Requirements and Certification

Refer to the system compatibility, requirements and certification documentation for information about hardware and software requirements, platforms, databases, and other information.

The compatibility documentation describes compatibility and interoperability considerations that may arise when you install, patch, or upgrade Oracle Fusion Middleware 12*c* components. For details, see *Understanding Interoperability and Compatibility*.

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

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

> **Note:**
>
> The Oracle Identity Management Integration components does not support the following operating systems:
>
> - AIX
> - HPUX Itanium
> - Microsoft Windows

For the latest requirements and certification documentation refer to the table "Oracle Fusion Middleware Certification Matrices" in the *Understanding Interoperability and Compatibility*.

1.7 Using My Oracle Support for Additional Troubleshooting Information

You can use My Oracle Support (formerly MetaLink) to help resolve Oracle Fusion Middleware problems.

My Oracle Support contains several useful troubleshooting resources, such as:

- Knowledge base articles
- Community forums and discussions
- Patches and upgrades
- Certification information

> **Note:**
>
> You can also use My Oracle Support to log a service request.

You can access My Oracle Support at `https://support.oracle.com`.

Part II
Core Integrations

This part describes integrations between certain IdM components.

This part contains the following chapter:

- Integrating Oracle Access Manager and LDAP
- Integrating Oracle Identity Governance with Oracle Access Manager and LDAP Connectors
- Troubleshooting Common Problems in Access Manager and OIG Integration
- Modifying OAM Configuration Properties

2

Integrating Oracle Access Manager and LDAP

Integrating Oracle Access Manager with LDAP involves preparing the IDStore, adding the missing object classes, and configuring OAM using automated script.

Topics include:

- Preparing IDStore Using Automated Script
- Adding Missing Object Classes Using Automated Script
- Configuring OAM Using Automated Script

2.1 Preparing IDStore Using Automated Script

Prepare IDStore using the `OIGOAMIntegration.sh` automated script for OIG-OAM integration.

Configure the identity store and policy store by creating the groups and setting ACIs to the various containers. Add necessary users and associating users with groups to the identity store. This step is similar to running the commands `idmConfigTool.sh -prepareIDStore` and `idmConfigTool.sh -prepareIDStore -mode=ALL`. See prepareIDStore Command.

1. Open the `prepareIDStore.all.config` file from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/config`) in a text editor and update the parameters.

   Example `prepareIDStore.all.config` File

```
IDSTORE_DIRECTORYTYPE: OID
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 3060
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_BINDDN_PWD: <password>
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_READONLYUSER: IDROUser
IDSTORE_READWRITEUSER: IDRWUser
IDSTORE_SUPERUSER: weblogic_fa
IDSTORE_OAMSOFTWAREUSER: oamLDAP
IDSTORE_OAMADMINUSER: oamAdmin
IDSTORE_OIMADMINUSER: oimLDAP
IDSTORE_OIMADMINGROUP: OIMAdministrators
IDSTORE_WLSADMINUSER: weblogic_idm
IDSTORE_WLSADMINGROUP: IDM Administrators
IDSTORE_OAAMADMINUSER: oaamAdminUser
```

```
## The domain for the email - e.g. user@example.com
IDSTORE_EMAIL_DOMAIN: company.com
POLICYSTORE_SHARES_IDSTORE: true
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
## If you are using OUD as the identity store, then the additional
properties are:
#IDSTORE_ADMIN_PORT: 4444
#IDSTORE_KEYSTORE_FILE: /u01/config/instances/oud1/OUD/config/admin-
keystore
## The value of the IDSTORE_KEYSTORE_PASSWORD parameter is the
content of the /u01/config/instances/oud1/OUD/config/admin-
keystore.pin
#IDSTORE_KEYSTORE_PASSWORD: <PASSWORD>
```

The following table describes the parameters that you can set in the `prepareIDStore.all.config` file.

Table 2-1 Parameters in `prepareIDStore.all.config` File

Property	Description	Sample Value
`IDSTORE_DIRECTORYTYPE`	Enter the identity store directory type. Valid options are OID, OUD, and AD.	`OID`
`IDSTORE_HOST`	Enter the identity store host name.	`idstore.example.com`
`IDSTORE_PORT`	Enter the identity store port.	`3060`
`IDSTORE_BINDDN`	An administrative user in Oracle Internet Directory, Oracle Unified Directory or Active Directory.	• OID: `cn=orcladmin` • OUD: `cn=oudadmin` • AD: `CN=Administrator,CN=Users,DC=example.com,DC=example,dc=com`
`IDSTORE_BINDDN_PWD`	Enter the Password for administrative user in Oracle Internet Directory, Oracle Unified Directory or Microsoft Active Directory.	*password*
`IDSTORE_USERNAMEATTRIBUTE`	Enter the `username` attribute used to set and search for users in the identity store.	`cn`
`IDSTORE_LOGINATTRIBUTE`	Enter the login attribute of the identity store that contains the user's login name.	`uid`
`IDSTORE_SEARCHBASE`	Enter the location in the directory where users and groups are stored.	`dc=example,dc=com`
`IDSTORE_USERSEARCHBASE`	Enter the Container under which Access Manager searches for the users.	`cn=users,dc=example,dc=com`
`IDSTORE_GROUPSEARCHBASE`	Enter the location in the directory where groups are stored.	`cn=groups,dc=example,dc=com`

Table 2-1 (Cont.) Parameters in `prepareIDStore.all.config` File

Property	Description	Sample Value
IDSTORE_SYSTEMIDBASE	Enter the location of a container in the directory where system-operations users are stored. There are only a few system operations users and are kept separate from enterprise users stored in the main user container. For example, the Oracle Identity Governance reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.	cn=systemids,dc=example,dc=com
IDSTORE_READONLYUSER	Enter the user with read-only permissions to the identity store.	IDROUser
IDSTORE_READWRITEUSER	Enter the user with read-write permissions to the identity store.	IDRWUser
IDSTORE_SUPERUSER	Enter the Oracle Fusion Applications superuser in the identity store.	weblogic_fa
IDSTORE_OAMSOFTWAREUSER	Enter the LDAP user that OAM uses to interact with LDAP.	oamLDAP
IDSTORE_OAMADMINUSER	Enter the user you use to access your Oracle Access Management Console.	oamAdmin
IDSTORE_OAMADMINUSER_PWD	Enter the password for the user you use to access your Oracle Access Management Console. **Note:** All password fields are optional. If you do not enter them in the file (security issues), then you are prompted to enter them when the script runs.	*password*
IDSTORE_OIMADMINUSER	Enter the user that Oracle Identity Governance uses to connect to the identity store.	oimLDAP
IDSTORE_OIMADMINUSER_PWD	Enter the Password for the user that Oracle Identity Governance uses to connect to the identity store.	*password*
IDSTORE_OIMADMINGROUP	Enter the group you want to create to hold your Oracle Identity Governance administrative users.	OIMAdministrators

Table 2-1 (Cont.) Parameters in `prepareIDStore.all.config` File

Property	Description	Sample Value
`IDSTORE_WLSADMINUSER`	Enter the identity store administrator for Oracle WebLogic Server.	`weblogic_idm` **Note:** This is default user name for the administrator user.
`IDSTORE_WLSADMINUSER_PWD`	Enter the password for Identity store administrator for Oracle WebLogic Server.	*password*
`IDSTORE_WLSADMINGROUP`	Enter the identity store administrator group for Oracle WebLogic Server.	`wlsadmingroup`
`IDSTORE_OAAMADMINUSER`	Enter the user you want to create as your Oracle Access Management Administrator. This user is created by the tool.	`oaamAdminUser`
`IDSTORE_XELSYSADMINUSER_PWD`	Enter the password of System administrator for Oracle Identity Goverance. Must match the value in Oracle Identity Governance	*password*
`POLICYSTORE_SHARES_IDSTORE`	Set it to `true` if your policy and identity stores are in the same directory. If not, it is set to `false`.	`TRUE`
`IDSTORE_ADMIN_PORT`	Enter the Administration port of your Oracle Unified Directory instance. If you are not using Oracle Unified Directory, you ignore this parameter.	`4444`
`IDSTORE_KEYSTORE_FILE`	Enter the location of the Oracle Unified Directory `Keystore` file. It is used to enable communication with Oracle Unified Directory using the Oracle Unified Directory administration port. It is called `admin-keystore` and is located in `OUD_ORACLE_INSTANCE/OUD/config`. If you are not using Oracle Unified Directory, you can ignore this parameter. This file must be located on the same host that the `OIGOAMIntegration.sh` command is running on. The command uses this file to authenticate itself with OUD.	`/u01/config/instances/oud1/OUD/config/admin-keystore`
`IDSTORE_KEYSTORE_PASSWORD`	Enter the encrypted password of the Oracle Unified Directory keystore. This value can be found in the file `OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin`. If you are not using Oracle Unified Directory, you can ignore this parameter.	*password*

2. Run the automated script for OIG-OAM integration to seed the directory with Users, Roles, and `ob` schema extensions.

```
OIGOAMIntegration.sh -prepareIDStore
```

> **Note:**
>
> In case of Active Directory, grant ACLs manually after executing `OIGOAMIntegration.sh -prepareIDStore` command. See Granting ACLs Manually for Active Directory

You have successfully executed the automated script for preparing the IDStore.

Verifying the Identity Store and Policy Store Configuration

Do the following in your LDAP directory:

- Search base for users and groups you specified in the `prepareIDStore.all.config` file exist in the LDAP directory.
- The user container, group container, and the System ID container exist in the LDAP directory.
- The `systemids` container includes the `IDROuser`, `IDRWUser`, `oamSoftwareUser`, and `oimadminuser` users. These are sample values provided in `prepareIDStore.all.config`. You can provide and use your own values.
- The user container includes the `oamadminuser`, `weblogic_fa`, `weblogic_idm`, and `xelsysadm` users. These are sample values provided in `prepareIDStore.all.config`. You can provide and use your own values.
- The group container includes the `OAMadministreatrs`, `OIMadminsitrators`, `BIReportAdminnistrator`, `Session REST API`, and `wlsadmingroup`, `orclFAGroup`, and `OAAM` groups.
- Access is granted to the changelog for OUD:

  If you are using Oracle Unified Directory, you must grant access to the `changelog` by performing the following steps on the single node LDAP host or on `LDAPHOST1` and `LDAPHOST2` for multinode LDAP instances:

  1. Create a file called `passwordfile` that contains the password you use to connect to OUD.

```
OUD_ORACLE_INSTANCE/OUD/bin/dsconfig set-access-control-handler-prop --remove \
global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version 3.0;
acl \"External changelog access\"; deny (all) userdn=\"ldap:///anyone\";)"  \
                --hostname OUD Host \
                --port OUD Admin Port \
                --trustAll \
                --bindDN cn=oudadmin \
                          --bindPasswordFile passwordfile \
                --no-prompt
```

  For example:

```
OUD_ORACLE_INSTANCE/OUD/bin/dsconfig set-access-control-handler-prop --remove \
global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version 3.0;
acl \"External changelog access\"; deny (all) userdn=\"ldap:///anyone\";)" \
```

```
                --hostname LDAPHOST1.example.com \
                   --port 4444 \
                --trustAll \
                --bindDN cn=oudadmin \
                --bindPasswordFile passwordfile \
                --no-prompt
```

2. Add the new act:

```
OUD_ORACLE_INSTANCE/OUD/bin/dsconfig set-access-control-handler-prop --
add \

global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version
3.0; acl \"External changelog access\"; allow
(read,search,compare,add,write,delete,export) groupdn=\"ldap:///
cn=OIMAdministrators,cn=groups,dc=example,dc=com\";)" \
                --hostname OUD Host \
                --port OUD Admin Port \
                --trustAll \
                --bindDN cn=oudadmin \
                --bindPasswordFile passwordfile \
                --no-prompt
```

For example:

```
OUD_ORACLE_INSTANCE/OUD/bin/dsconfig set-access-control-handler-prop --
add \
global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version
3.0; acl \"External changelog access\"; allow
(read,search,compare,add,write,delete,export) groupdn=\"ldap:///
cn=OIMAdministrators,cn=groups,dc=example,dc=com\";)" \
                      --hostname LDAPHOST1.example.com \
             --port 4444 \
             --trustAll \
             --bindDN cn=oudadmin \
             --bindPasswordFile passwordfile \
             --no-prompt
```

- Additional OUD grants are created:

  Update *OUD_ORACLE_INSTANCE*/OUD/config/config.ldif on all OUD instances with below changes:

  1. Look at the following line:

```
ds-cfg-global-aci: (targetcontrol="1.3.6.1.1.12 || 1.3.6.1.1.13.1 ||
1.3.6.1.1.13.2 || 1.2.840.113556.1.4.319 || 1.2.826.0.1.3344810.2.3 ||
2.16.840.1.113730.3.4.18 || 2.16.840.1.113730.3.4.9 ||
1.2.840.113556.1.4.473 || 1.3.6.1.4.1.42.2.27.9.5.9") (version 3.0; acl
"Authenticated users control access"; allow(read) userdn="ldap:///all";)
```

  Remove the Object Identifier 1.2.840.113556.1.4.319 from the above aci and add it to following aci as shown:

```
ds-cfg-global-aci: (targetcontrol="2.16.840.1.113730.3.4.2 ||
2.16.840.1.113730.3.4.17 || 2.16.840.1.113730.3.4.19 ||
1.3.6.1.4.1.4203.1.10.2 || 1.3.6.1.4.1.42.2.27.8.5.1 ||
2.16.840.1.113730.3.4.16 || 2.16.840.1.113894.1.8.31 ||
1.2.840.113556.1.4.319") (version 3.0; acl "Anonymous control access";
allow(read) userdn="ldap:///anyone";)
```

  2. Add Object Identifiers 1.3.6.1.4.1.26027.1.5.4 and 1.3.6.1.4.1.26027.2.3.4 to the following aci as shown:

```
ds-cfg-global-aci: (targetcontrol="1.3.6.1.1.12 || 1.3.6.1.1.13.1 ||
1.3.6.1.1.13.2 || 1.2.826.0.1.3344810.2.3 || 2.16.840.1.113730.3.4.18 ||
2.16.840.1.113730.3.4.9 || 1.2.840.113556.1.4.473 || 1.3.6.1.4.1.42.2.27.9.5.9
|| 1.3.6.1.4.1.26027.1.5.4 || 1.3.6.1.4.1.26027.2.3.4") (version 3.0; acl
"Authenticated users control access"; allow(read) userdn="ldap:///all";)
```

3. Restart the Oracle Unified Directory server on both LDAPHOSTs.

- Additional OUD indexes are created:

  When you ran the `OIGOAMIntegration.sh -prepareIDStore` script to prepare an OUD identity store, it creates indexes for the data on the instance against which it is run. These indexes must be manually created on each of the OUD instances in LDAPHOST2. To do this, run the following commands on LDAPHOST2:

```
OUD_ORACLE_INSTANCE/OUD/bin/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444 -a -
D "cn=oudadmin" -j passwordfile -c \-f IAD_ORACLE_HOME/idm/oam/server/oim-intg/
ldif/ojd/schema/ojd_user_index_generic.ldif

OUD_ORACLE_INSTANCE/OUD/bin/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444 -a -
D "cn=oudadmin" -j  passwordfile -c \-f IAD_ORACLE_HOME/idm/idmtools/templates/oud/
oud_indexes_extn.ldif
```

Granting ACLs Manually for Active Directory

For Active Directory, after running `OIGOAMIntegration.sh -prepareIDStore`, perform the following on the AD server machine:

1. Add ACLs.

```
dsacls /G cn=orclFAUserReadPrivilegeGroup,<IDSTORE_GROUPSEARCHBASE>:GR
dsacls /G cn=orclFAUserWritePrivilegeGroup,<IDSTORE_GROUPSEARCHBASE>:GW
dsacls /G cn=orclFAGroupReadPrivilegeGroup,<IDSTORE_GROUPSEARCHBASE>:GR
dsacls /G cn=orclFAGroupWritePrivilegeGroup,<IDSTORE_GROUPSEARCHBASE>:GW
dsacls /G cn=orclFAOAMUserWritePrivilegeGroup,<IDSTORE_GROUPSEARCHBASE>:GW
```

2. Reset User Password.

```
dsmod user "CN=weblogic_idm,<IDSTORE_USERSEARCHBASE>" -pwd <password> -mustchpwd no
dsmod user "CN=xelsysadm,<IDSTORE_USERSEARCHBASE>" -pwd <password> -mustchpwd no
dsmod user "CN=oamadmin,<IDSTORE_USERSEARCHBASE>" -pwd <password> -mustchpwd no
dsmod user "CN=OblixAnonymous,DC=interop,DC=example,DC=com" -pwd <password> -
mustchpwd no
dsmod user "CN=oamLDAP,<IDSTORE_SYSTEMIDBASE>" -pwd <password> -mustchpwd no
dsmod user "CN=oimLDAP,<IDSTORE_SYSTEMIDBASE>" -pwd <password> -mustchpwd no
```

3. Enable user accounts.

```
dsmod user "CN=weblogic_idm,<IDSTORE_USERSEARCHBASE>" -disabled no
dsmod user "CN=xelsysadm,<IDSTORE_USERSEARCHBASE>" -disabled no
dsmod user "CN=oamadmin,<IDSTORE_USERSEARCHBASE>" -disabled no
dsmod user "CN=OblixAnonymous,DC=interop,DC=example,DC=com" -disabled no
dsmod user "CN=oamLDAP,<IDSTORE_SYSTEMIDBASE>" -disabled no
dsmod user "CN=oimLDAP,<IDSTORE_SYSTEMIDBASE>" -disabled no
```

2.2 Adding Missing Object Classes Using Automated Script

Add the Missing Object Classes using the `OIGOAMIntegration.sh` automated script.

When you prepare your LDAP directory for use with Oracle Access Manager, it extends the directory schema to include a number of specific object classes, which are used by Oracle Access Manager.

After the object classes are added, any new users created in the directory are automatically assigned these object classes. Once the object classes are added to the directory, it is important to ensure that any existing users also have these new object classes so that they can be successfully managed with Oracle Access Manager.

The `OIGOAMIntegration.sh` script checks each user in the LDAP directory to ensure that they have all of the recommended object classes.

To add the Missing Object Classes:

> **Note:**
>
> You can only add object classes for existing users in Oracle Internet Directory or Oracle Unified Directory. This feature is not supported in Active Directory.

1. Open the `addMissingObjectClasses.config` file from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/config`) in a text editor and update the parameters.

   Example `addMissingObjectClasses.config` File

   ```
   IDSTORE_DIRECTORYTYPE: OID
   IDSTORE_HOST: idstore.example.com
   IDSTORE_PORT: 3060
   IDSTORE_BINDDN: cn=orcladmin
   IDSTORE_BINDDN_PWD: <password>
   IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
   ```

   The following table describes the parameters that you can set in the `addMissingObjectClasses.config` file.

Table 2-2 Parameters in addMissingObjectClasses.config file

Parameters	Description	Sample Value
`IDSTORE_DIRECTORYTYPE`	Enter the identity store directory type. Valid options are OID or OUD.	`OUD`
`IDSTORE_HOST`	Enter the identity store host name.	`idstore.example.com`
`IDSTORE_PORT`	Enter the identity store port.	`389`
`IDSTORE_BINDDN`	An administrative user in Oracle Internet Directory or Oracle Unified Directory.	• OID: `cn=orcladmin` • OUD: `cn=oudadmin`
`IDSTORE_BINDDN_PWD`	Enter the password for administrative user in Oracle Internet Directory or Oracle Unified Directory.	*password*
`IDSTORE_USERSEARCHBASE`	Enter the location in the directory where users are stored.	`cn=users,dc=example,dc=com`

2. Run the `OIGOAMIntegration.sh` script from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/bin`) to enable OAM notifications:

   ```
   OIGOAMIntegration.sh -addMissingObjectClasses
   ```

You have successfully executed the automated script to add object classes for existing users in LDAP directory.

> **Note:**
>
> This step depends on the number of users in the LDAP directory. It is estimated to take 10 minutes per 10000 users in the LDAP directory.

If there are no object classes in the LDAP, then the following are added for the existing LDAP users:

- `OIMPersonPwdPolicy`
- `OblixOrgPerson`
- `OblixPersonPwdPolicy`
- `obpasswordexpirydate`

2.3 Configuring OAM Using Automated Script

Configure Oracle Access Manager using the `OIGOAMIntegration.sh` automated script.

1. Open the `configOAM.config` file from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/config`) in a text editor and update the parameters.

   Example `configOAM.config` File

   ```
   WLSHOST: oamadminhost.example.com
   WLSPORT: 7001
   WLSADMIN: weblogic
   IDSTORE_HOST: idstore.example.com
   IDSTORE_PORT: 3060
   IDSTORE_BINDDN: cn=orcladmin
   IDSTORE_USERNAMEATTRIBUTE: cn
   IDSTORE_LOGINATTRIBUTE: uid
   IDSTORE_SEARCHBASE: dc=example,dc=com
   IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
   IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
   IDSTORE_OAMSOFTWAREUSER: oamLDAP
   IDSTORE_OAMADMINUSER: oamAdmin
   PRIMARY_OAM_SERVERS: oamhost1.example.com:5575,oamhost2.example.com:5575
   WEBGATE_TYPE: ohsWebgate11g
   ACCESS_GATE_ID: Webgate_IDM
   OAM11G_IDM_DOMAIN_OHS_HOST: sso.example.com
   OAM11G_IDM_DOMAIN_OHS_PORT: 443
   OAM11G_IDM_DOMAIN_OHS_PROTOCOL: https
   OAM11G_OAM_SERVER_TRANSFER_MODE: Open
   OAM11G_IDM_DOMAIN_LOGOUT_URLS: /console/jsp/common/logout.jsp,/em/
   ```

```
targetauth/emaslogout.jsp
OAM11G_WG_DENY_ON_NOT_PROTECTED: false
OAM11G_SERVER_LOGIN_ATTRIBUTE: uid
OAM_TRANSFER_MODE: Open
COOKIE_DOMAIN: .example.com
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
OAM11G_SSO_ONLY_FLAG: true
OAM11G_OIM_INTEGRATION_REQ: true
OAM11G_IMPERSONATION_FLAG: true
OAM11G_SERVER_LBR_HOST: sso.example.com
OAM11G_SERVER_LBR_PORT: 443
OAM11G_SERVER_LBR_PROTOCOL: https
COOKIE_EXPIRY_INTERVAL: 120
OAM11G_OIM_OHS_URL: https://sso.example.com:443/
SPLIT_DOMAIN: true
OAM11G_IDSTORE_NAME: OAMIDSTORE
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
```

The following table describes the parameters that you can set in the `configOAM.config` file.

Table 2-3 Parameters in `configOAM.config` File

Property	Description	Sample Value
`ACCESS_GATE_ID`	Name, with which WebGate profile gets created. Its artifacts are available under `<DOMAIN_HOME>/Output/<ACCESS_GATE_ID>` This is the value specified during OAM configuration.	`Webgate_IDM`
`COOKIE_DOMAIN`	Enter the domain in which the WebGate functions.	`.example.com`
`COOKIE_EXPIRY_INTERVAL`	Enter the Cookie expiration period.	`120`
`IDSTORE_BINDDN`	An administrative user in Oracle Internet Directory, Oracle Unified Directory or Active Directory.	• OID: `cn=oracladmin` • OUD: `cn=oudadmin` • Active Directory: `CN=Administrator,CN=Users,DC=example.com,DC=example,dc=com`
`IDSTORE_GROUPSEARCHBASE`	Enter the location in the directory where groups are stored.	`cn=groups,dc=example,dc=com`

Table 2-3 (Cont.) Parameters in `configOAM.config` File

Property	Description	Sample Value
IDSTORE_HOST	Enter the identity store host name.	idstore.example.com
IDSTORE_LOGINATTRIBUTE	Enter the login attribute of the identity store that contains the user's login name.	uid
IDSTORE_OAMADMINUSER	Enter the user you use to access your Oracle Access Management Console.	oamAdmin
IDSTORE_OAMSOFTWAREUSER	Enter the user you use to interact with the LDAP server.	oamLDAP
IDSTORE_PORT	Enter the identity store port.	389
IDSTORE_SEARCHBASE	Enter the location in the directory where users and groups are stored.	dc=example,dc=com
IDSTORE_SYSTEMIDBASE	Enter the location of a container in the directory where system-operations users are stored. There are only a few system operations users and are kept separate from enterprise users stored in the main user container. For example, the Oracle Identity Governance reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.	cn=systemids,dc=example,dc=com
IDSTORE_USERNAMEATTRIBUTE	Enter the `username` attribute used to set and search for users in the identity store.	cn
IDSTORE_USERSEARCHBASE	Enter the Container under which Access Manager searches for the users.	cn=users,dc=example,dc=com
OAM_TRANSFER_MODE	Enter the security mode in which the access servers function. Supported values are `OPEN` and `SIMPLE` Oracle recommends using SIMPLE. **Note:** If you change the security mode from Open, then update the existing agents to use the new mode.	SIMPLE
OAM11G_IDM_DOMAIN_LOGOUT_URLS	Set to the various logout URLs.	/console/jsp/common/logout.jsp,/em/targetauth/emaslogout.jsp
OAM11G_IDM_DOMAIN_OHS_HOST	Enter the load balancer that is in front of Oracle HTTP Server (OHS) in a high-availability configuration.	login.example.com

Table 2-3 (Cont.) Parameters in `configOAM.config` File

Property	Description	Sample Value
`OAM11G_IDM_DOMAIN_OHS_PORT`	Enter the load balancer port.	`443`
`OAM11G_IDM_DOMAIN_OHS_PROTOCOL`	Enter the Protocol to use when directing requests to the load balancer.	`https`
`OAM11G_IDSTORE_NAME`	Enter the name of the identity store configured in OAM. This will be set as the default/System ID Store in OAM.	`OAMIDSTORE`
`OAM11G_IDSTORE_ROLE_SECURITY_ADMIN`	Account to administer role security in identity store.	`OAMAdministrators`
`OAM11G_IMPERSONATION_FLAG`	It enables or disables the impersonation feature in the OAM Server.	`true`
`OAM11G_OAM_SERVER_TRANSFER_MODE`	Enter the security mode in which the access servers function. Supported values are `OPEN` and `SIMPLE`	`Open`
`OAM11G_OIM_INTEGRATION_REQ`	It specifies whether to integrate with Oracle Identity Governance or configure Access Manager in stand-alone mode. Set to `true` for integration. If you set this value to false and then add Oracle Identity Governance at a later stage, then you can rerun this script with the value set to true. This parameter controls whether or not the Oracle Identity Governance Register User, Track Requests, and Forgotten Password links are included in the Oracle Access Manager login page.	`true`
`OAM11G_OIM_OHS_URL`	Enter the URL of the load balancer or Oracle HTTP Server (OHS) fronting the OIM server.	`https://oig.example.com:443/`
`OAM11G_SERVER_LBR_HOST`	Enter the OAM Server fronting your site.	`login.example.com`
`OAM11G_SERVER_LBR_PORT`	Enter the port that the load balancer is listening on (*`HTTP_SSL_PORT`*).	`443`
`OAM11G_SERVER_LBR_PROTOCOL`	Enter the Protocol to use when directing requests to the load balancer.	`https`
`OAM11G_SERVER_LOGIN_ATTRIBUTE`	Setting to `uid` ensures the validation of the username against the uid attribute in LDAP when the user logs in.	`uid`
`OAM11G_SSO_ONLY_FLAG`	Set it to configure Access Manager 11g as authentication only mode or normal mode, which supports authentication and authorization. Default value is `true`. If value is set to `false`, access is denied to protected resources for any users.	`true`
`OAM11G_WG_DENY_ON_NOT_PROTECTED`	Set to deny on protected flag for 10g WebGate. Valid values are `true` and `false`. Set the value to `true` as a best practice.	`true`

Table 2-3 (Cont.) Parameters in `configOAM.config` File

Property	Description	Sample Value
PRIMARY_OAM_SERVERS	Enter comma-separated list of your Access Manager servers and the proxy ports they use.	oamhost1.example.com:5575, oamhost2.example.com:5575
SPLIT_DOMAIN	Set to `true` is required to suppress the double authentication of Oracle Access Management Console.	true
WEBGATE_TYPE	Enter the WebGate agent type you want to create. 10g is no longer supported in 12c.	ohsWebgate12c
WLSADMIN	Enter the WebLogic Server administrative user account you use to log in to the WebLogic Server Administration Console in OAM domain.	weblogic
WLSHOST	Enter the Administration server host name in OAM domain.	oamadminhost.example.com
WLSPORT	Enter the Administration server port in OAM domain.	7001

2. Stop the policy server. See Starting and Stopping Managed WebLogic Servers and Access Manager Servers.
3. Set the `MW_HOME` environment variable to OIG Middleware.
4. Run the automated script for OIG-OAM integration to configure OAM.

   ```
   OIGOAMIntegration.sh -configOAM
   ```

   You have successfully executed the automated script for configuring Oracle Access Manager.
5. Restart the OAM domain servers. See Starting and Stopping Managed WebLogic Servers and Access Manager Servers.

Verifying the OAM Configuration

You can verify the OAM configuration by performing the following steps:

1. When Single Sign-on is implemented, provide the LDAP group IDM Administrators with WebLogic administration rights, so that you can log in using one of these accounts and perform WebLogic administrative actions. To add the LDAP Groups OAMAdministrators and WLSAdministrators to the WebLogic Administrators:
   a. Log in to the WebLogic Administration Server Console as the default administrative user. For example, `weblogic`.
   b. In the left pane of the console, click **Security Realms**.
   c. On the Summary of Security Realms page, click **myrealm** under the Realms table.
   d. On the Settings page for myrealm, click the **Roles & Policies** tab.
   e. On the Realm Roles page, expand the **Global Roles** entry under the Roles table.
   f. Click the **Roles** link to go to the Global Roles page.

g. On the Global Roles page, click the **Admin** role to go to the Edit Global Roles page.

h. On the Edit Global Roles page, under the **Role Conditions** table, click the **Add Conditions** button.

i. On the Choose a Predicate page, select **Group** from the drop down list for predicates and click **Next**.

j. On the Edit Arguments Page, Specify **OAMAdministrators** in the **Group Argument** field and click **Add**.

k. Repeat for the group **WLSAdministrators**.

l. Click **Finish** to return to the Edit Global Roles page.

m. The Role Conditions table now shows the groups **OAMAdministrators or WLSAdministrators** as role conditions.

n. Click **Save** to finish adding the Admin role to the OAMAdministrators and IDM Administrators Groups.

2. Search for the WebGate name that you specified in the `configOAM.config` properties file:

   a. Log in to the Oracle Access Management Console as the OAM admin user:

   `http://oam_adminserver_host:oam_adminserver_port/oamconsole`

   b. From the **Application Security** Launch Pad, click **Agents**.

   The Search SSO Agents page is displayed.

   c. In the **Search** field, enter the WebGate name.

   > **Note:**
   >
   > This is the value you specified for `ACCESS_GATE_ID` in the `configOAM.config` properties file.

   d. In the Search Result Table, you can see the agent.

3. Verify that the name of the identity store you specified in the `configOAM.config` file is automatically selected as the default store:

   - Click the **Configuration** Launch Pad and select **User Identity Stores**.
   - In the Default and System Store section, verify that the name of the identity store you specified in the `configOAM.config` file (For example, `OAMIDSTORE`) is selected as the Default Store and System Store.

4. For a clustered deployment, perform the following steps:

   a. In the OAM Console, click the **Agents** pad on the Application Security screen.

   b. Ensure that the **WebGates** tab is selected.

   c. Click **Search**.

   d. Click an Agent, for example: **IAMSuiteAgent**.

   e. Set the Security value to the same value defined to OAM Transfer Mode on the Access Manager Configuration screen during response file creation.

If you have changed the OAM security model using the `OIGOAMIntegration` tool, change the security model used by any existing Webgates to reflect this change.

Click **Apply**.

f. In the Primary Server list, click **+**, and add any missing Access Manager Servers.

g. If a password has not already been assigned, enter a password into the **Access Client Password** field, and click **Apply**.

Assign an Access Client Password, such as the **Common IAM Password** (`COMMON_IDM_PASSWORD`) you used during the response file creation or an Access Manager-specific password, if you have set one.

h. Set **Maximum Connections** to 20. This is the total maximum number of connections for the primary servers, which is 10 x WLS_OAM1 connections plus 10 x WLS_OAM2 connections.

i. If you see the following in the **User Defined Parameters** or the **Logout redirect URL**:

```
logoutRedirectUrl=http://OAMHOST1.example.com:14100/oam/server/logout
```

Change it to:

```
logoutRedirectUrl=https://login.example.com/oam/server/logout
```

j. Click **Apply**.

k. Repeat the steps a through j for each WebGate.

l. Check that the security setting matches that of your Access Manager servers.

3

Integrating Oracle Identity Governance with Oracle Access Manager and LDAP Connectors

Integrate Oracle Identity Governance (OIG) with Oracle Access Manager (OAM) and LDAP Connectors. You can run an automated integration script to complete OIG-OAM integration or perform configuration operations individually. The script utilizes user-supplied values from property files to perform various configurations.

This chapter provides step-by-step instructions for integrating Oracle Access Manager (Access Manager) and Oracle Identity Governance (Enterprise Edition). Use the automated script for integration if your integrated environment includes LDAP Connectors and any third-party access product. Also you can perform this integration incrementally. When you run each task in the automated integration script separately to complete OIG-OAM integration, you can evaluate the result of each successive step. Rerun the step, if required, or proceed to the next step in the sequence until all steps are successfully completed.

> **Note:**
>
> The exact details in this chapter may differ depending on your specific deployment. Adapt information as required for your environment.
>
> This chapter covers the steps to integrate Oracle Identity Governance with Oracle Access Manager and LDAP. It does not cover integrating Oracle Access Manager with LDAP. If you are creating a fully integrated environment, then you should perform the steps in Integrating Oracle Access Manager and LDAP prior to performing the integration steps in this chapter.

The integration instructions assume Identity Governance components have been configured on separate Oracle WebLogic domains, as discussed in About the Basic Integration Topology. For prerequisite and detailed information on how the components were installed and configured in this example integration, see Preparing to Install and Configure Oracle Identity and Access Management in *Fusion Middleware Installing and Configuring Oracle Identity and Access Management*

If you are deploying Oracle Identity Governance components in an enterprise integration topology, as discussed in About the Basic Integration Topology, see Understanding an Enterprise Deployment in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management* for implementation procedures.

This chapter contains these sections:

- Overview of Oracle Identity Governance and Access Manager Integration
- Configuring Oracle Identity Governance and Oracle Access Manager Integration
- Validating the Access Manager and Oracle Identity Governance Integration

3.1 Overview of Oracle Identity Governance and Oracle Access Manager Integration

This integration scenario enables you to manage identities with Oracle Identity Governance and control access to resources with Oracle Access Manager. Oracle Identity Governance is a user provisioning and administration solution that automates user account management, whereas Access Manager provides a centralized and automated single sign-on (SSO) solution.

This section contains the following topics:

3.1.1 About Integrating Oracle Identity Governance with Oracle Access Manager

In the Oracle Access Manager (OAM) and Oracle Identity Governance (OIG) integration, users have the capability to:

- Create and reset the password without assistance for expired and forgotten passwords
- Recover passwords using challenge questions and answers
- Set up challenge questions and answers
- Perform self-service registration
- Perform self-service profile management
- Access multiple applications securely with one authentication step

See About Password Management Scenarios.

3.1.2 About Oracle Identity Governance and Oracle Access Manager Single-Node Integration Topology

You must configure IdM components, Access Manager and Oracle Identity Governance, in separate WebLogic Server domains (split domain topology), as discussed in About the Basic Integration Topology, and separate Oracle Middleware homes. Otherwise, attempts to patch or upgrade one product may be blocked by a version dependency on a component shared with another. When you install Oracle Identity Governance components in a single WebLogic Server domain, there is a risk

that the component (libraries, jars, utilities, and custom plug-ins) you are installing into the domain might not be compatible with other components, thereby resulting in problems across your entire domain.

Access Manager uses a database for policy data and a directory server for identity data. This integration scenario assumes a single directory server. The directory server must also be installed in a separate domain and a separate Middleware home as well.

> **Note:**
>
> The instructions in this chapter assume that you will use Oracle Unified Directory as the identity store.

3.1.3 Prerequisites to Integrating Oracle Identity Governance and Oracle Access Manager

Ensure the required environment is set and made available for the integration.

> **Note:**
>
> You can upgrade the existing 11*g* and 12*c* OIG and OAM integrated environments to the latest 12c (12.2.1.4.0) release version. For more information, see Upgrading OIG-OAM Integrated Environments.

In the following sections it is assumed that the required components, as listed in Table 3-1, have already been installed, including any dependencies, and the environment is configured prior to the integration. See Understanding Oracle Identity Management Integration Topologies.

> **Note:**
>
> - Use 12.2.1.4.0 binaries for OAM and OIG.
> - OUD needs to have the changelog enabled for incremental reconciliation from OIG to work. If this is not enabled, the incremental reconciliation will not work. On a replicated OUD instance, `cn=changelog` is available by default depending on the condition that this instance contains both directory server and replication server components, which is the default. The changelog has no additional cost since the replication is already up.
>
>   On a non replicated OUD instance, `cn=changelog` is not available by default because there is a cost in disk and cpu that should not be paid if it is not useful. This can be easily enabled with the following command:
>
>   ```
>   $ dsreplication enable-changelog -h localhost -p 4444 -D "cn=directory
>   manager" -r 8989 -b "dc=example,dc=com"
>   ```

Table 3-1 Required Components for Integration Scenario

Component	Information
Oracle HTTP Server with Oracle HTTP Server WebGate	Oracle HTTP Server with Oracle HTTP Server WebGate is installed. Oracle Webgate is used to ensure that users are permitted to perform the actions that they are requesting. Oracle Access Manager is responsible for checking that the user has logged in, and that they are permitted to access the resources (URL's) that they are requesting. To ensure that all traffic is authorised, all traffic must go through a Web Proxy server, which has Oracle Webgate installed. For more information, see Installing Oracle HTTP Server and Configuring the Oracle HTTP Server WebGate.
Oracle SOA Suite	Oracle Identity Governance requires Oracle SOA Suite 12.2.1.4.0, which is exclusive to Oracle Identity and Access Management. SOA Suite is a prerequisite for Oracle Identity Governance and must be installed in the same domain as Oracle Identity Governance. If you use SOA Suite for other purposes, a separate install must be set up for running your own services, composites, BPEL processes, and so on. For more information, see Installing and Configuring the Oracle Identity Governance Software in *Installing and Configuring Oracle Identity and Access Management*.
Oracle Unified Directory	Oracle Unified Directory or Oracle Internet Directory or Microsft Active Directory is installed. See Installing the Oracle Unified Directory Software in *Installing Oracle Unified Directory*.
Access Manager	Access Manager is already installed and bundle patch 12.2.1.4.191223 applied or the latest bundle patch available for your release. See: • Installing and Configuring the Oracle Access Management Software in *Installing and Configuring Oracle Identity and Access Management*. • For the latest bundle patch, visit the Oracle Identity Management website at: https://docs.oracle.com/en/middleware/idm/suite/12.2.1.4/bundlepatch.html **Note:** If you are upgrading to the 12*c* (12.2.1.4.0) release version, then the OAM bundle patch 12.2.1.4.200327 applied or the latest bundle patch available for your release. For more information about upgrade, see Upgrading OIG-OAM Integrated Environments.

Table 3-1 (Cont.) Required Components for Integration Scenario

Component	Information
Oracle Identity Governance	Oracle Identity Governance 12.2.1.4.0 is already installed and the latest bundle patch for your release is applied. See Installing and Configuring the Oracle Identity Governance Software in *Installing and Configuring Oracle Identity and Access Management*.
Environmental Variables	Set the environmental variables required for OIG-OAM integration. See Set Up Environment Variables for OIG-OAM Integration.

Note:

If you are upgrading to the 12*c* (12.2.1.4.0) release version, then the OIM bundle patch 12.2.1.4.200505 applied or the latest bundle patch available for your release.

For more information about upgrade, see Upgrading OIG-OAM Integrated Environments.

See Also:

Prerequisites for the Connector-based Integration

3.1.4 Roadmap to Integrating Oracle Identity Governance and Oracle Access Manager

Table 3-2 lists the high-level tasks for integrating Access Manager and Oracle Identity Governance with Oracle Unified Directory.

Depending on your installation path, you may already have performed some of the integration procedures listed in this table. For details on the installation roadmap, see Understanding the Installation Roadmap.

Table 3-2 Integration Flow for Access Manager and Oracle Identity Governance

No.	Task	Information
1	Verify that all required components have been installed and configured prior to integration.	See Prerequisites to Integrating Oracle Identity Governance and Oracle Access Manager
2	Install Oracle HTTP Server and configuring the Oracle HTTP Server WebGate with Oracle Access Manager.	See Installing Oracle HTTP Server and Configuring the Oracle HTTP Server WebGate.
3	Integrate Oracle Access Manager with LDAP	See Integrating Oracle Access Manager and LDAP

Table 3-2 (Cont.) Integration Flow for Access Manager and Oracle Identity Governance

No.	Task	Information
4	Integrate Access Manager and Oracle Identity Governance.	See Configuring Oracle Identity Governance and Oracle Access Manager Integration

> **Note:**
>
> If you are adding OIG to an existing OAM/LDAP integrated environment that previously did not have OIG, then add the OIG links to the OAM login page. To do this, rerun the step Configuring OAM Using Automated Script with the parameter `OAM11G_OIM_INTEGRATION_REQ` set to `true`.

Table 3-2 (Cont.) Integration Flow for Access Manager and Oracle Identity Governance

No.	Task	Information
5	Stop the Oracle WebLogic Server managed servers for Access Manager and Oracle Identity Governance.	See Starting and Stopping Admin Server in *Administering Oracle Fusion Middleware*
6	Test the integration.	See Validating the Access Manager and Oracle Identity Governance Integration

3.2 Installing Oracle HTTP Server and Configuring the Oracle HTTP Server WebGate

Oracle HTTP Server WebGate is a Web server plug-in that intercepts HTTP requests and forwards them to an Oracle Access Management instance for authentication and authorization.

To install the Oracle HTTP Server and configuring the Oracle HTTP Server WebGate, do the following:

1. Install the Oracle HTTP Server in collocated mode.

   > **Note:**
   >
   > - Ensure that you select **Collocated HTTP Server (Managed through WebLogic server)** as the Installation Type during the installation process.
   > - OHS can be installed and configured as extended domain or setup as separate domain.

   For more information, see Installing the Oracle HTTP Server Software in *Installing and Configuring Oracle HTTP Server*.

2. Update the Oracle Access Management domain with Oracle HTTP Server.

   For more information about extending the existing Oracle Access Management domain with Oracle HTTP Server, see Configuring Oracle HTTP Server in a Collocated Domain in *Installing and Configuring Oracle HTTP Server*.

   > **Note:**
   >
   > Ensure that you add the Oracle Access Management machine and assign the Oracle HTTP Server instance to the selected machine in the Assign System Components to Machines screen during the configuration process.

3. Configure Oracle HTTP Server WebGate for Oracle Access Manager. For more information, see Configuring Oracle HTTP Server WebGate for Oracle Access Manager in *Installing WebGates for Oracle Access Manager*.

3.3 Configuring Oracle Identity Governance and Oracle Access Manager Integration

The automated script for integration simplifies the process of a connector-based integration between Oracle Identity Governance (OIG) and Oracle Access Manager (OAM) or any third-party access product. You can integrate OIG and OAM with directories such as Oracle Unified Directory (OUD), Oracle Internet Directory (OID) and Active Directory (AD).

This chapter contains the following topics:

- Prerequisites for the Connector-based Integration
- Step-by-step Procedure for OIG-OAM Integration Using Automated Script

3.3.1 Prerequisites for the Connector-based Integration

Prepare the environment ready for the connector-based integration using the automated integration script. Ensure that the system-level requirements are met, 12.2.1.4.0 binaries are installed, and the required connector is downloaded.

Verifying the Environment

- Check that your operating system is up-to-date with all necessary patches applied.
- Mount the binaries you will be using. The applicable Oracle software includes:
  - Oracle Database 12c (12.2.x.x)
  - JRF 12.2.1.4.0
  - Oracle Identity and Access Management 12*c* (12.2.1.4.0)
  - Oracle Unified Directory 12*c* (12.2.1.4.0) /Oracle Internet Directory 12*c* (12.2.1.4.0)
  - Oracle Fusion Middleware Infrastructure 12*c* (12.2.1.4.0)

> **Note:**
>
> - Use 12.2.1.4.0 binaries for OAM and OIG.
> - Apply OAM bundle patch 12.2.1.4.191223 or the latest bundle patch available for your release before starting the integrating process.
> - If you are upgrading OAM-OIG integrated environments from 11g Release 2 (11.1.2.3.0) or 12c (12.2.1.3.0) to the latest 12c (12.2.1.4.0) release version, then apply the following bundle patches:
>   * OAM bundle patch 12.2.1.4.200327
>   * OIM bundle patch 12.2.1.4.200505
> - The Oracle HTTP Server with 12*c* WebGate must be installed.

- Verify that Oracle Database is connected and accessible.

- Verify that the directory of your choice (OUD/OID/AD) is up and running.
- Verify that Oracle Access Manager is up and running.
- Verify that Oracle Access Manager is integrated with LDAP, as described in Integrating Oracle Access Manager and LDAP.
- Verify that Oracle Identity Governance is up and running.
- Verify if the environmental variables are set, as described in Set Up Environment Variables for OIG-OAM Integration.
- Ensure that Oracle Access Manager and Oracle Identity Governance are installed on separate domains.

> **Note:**
>
> The automated integration script, `OIGOAMIntegration.sh` works with OIG and OAM on separate hosts and domains. It is not required to have OIG and OAM on the same domain.

- Perform one of the following:
  - If you are using Oracle Linux 8 (OEL 8) or Red Hat Enterprise Linux 8 (RHEL 8) operating systems then install `tmux` before running the `OIGOAMIntegration.sh` script.

    The `tmux` package is already available in OEL 8/RHEL 8. For example, you can run the following command to install the `tmux` package.

    ```
    yum install tmux
    ```

  - If you are using operating systems older than or other than OEL 8/RHEL 8, ensure that the screen package is installed on your server by running the following command:

    ```
    rpm -qa | grep screen
    ```

    The command returns the value as shown in the following example:

    ```
    screen.x86_64 0:4.1.0-0.23.20120314git3c2946.el7_2
    ```

    If the command does not return information about the screen package version then install the package as follows:

    1. Log on to your Linux server as root
    2. Run `yum install screen` to install the screen package (For example, `screen.x86_64 0:4.1.0-0.23.20120314git3c2946.el7_2`):

       ```
       [root@server]# yum install screen
       > Package screen.x86_64 0:4.1.0-0.23.20120314git3c2946.el7_2 will
       be
       installed
       Total download size: 552 k
       Installed size: 914 k
       Is this ok [y/d/N]:
       ```

```
Enter 'y' and press enter.

Downloading packages:
screen-4.1.0-0.23.20120314git3c2946.el7_2.x86_64.rpm

Installed:
screen.x86_64 0:4.1.0-0.23.20120314git3c2946.el7_2
```

- Ensure that the OpenLDAP packages are installed:

  ```
  yum install openldap openldap-clients
  ```

  Verify if the version is on your system by entering the command `which ldapsearch`. The command returns the value as shown in the following example:

  ```
  /usr/bin/ldapsearch
  ```

  Update your `$PATH` to the LDAP directory server installation directory.

Updating Datasource Related to OIG Metadata Services (MDS) Configuration

1. Log in to the WebLogic Administrative Console for OIG.
2. In the left pane, under Domain Structure, expand **Services**, and then click **Data Sources**.
3. Click **mds-oim**, click the **Connection Pool** tab.
4. Update the following property values in the MDS-OIM connection pool:
   - Initial Capacity to 50
   - Maximum Capacity to 150
   - Minimum Capacity to 50
5. To update the value for **Inactive Connection Timeout**:

   In the same datasource, click **Advanced** link under the bottom of the page and set the **Inactive Connection Timeout** value to `10`.
6. Click **Save**.
7. Click **Activate Changes**.

Downloading the Connector

1. Download the Connector bundle from the artifactory: Download Connector Bundle
   - For OID or OUD, download the `oid-12.2.1.3.0.zip` Connector bundle corresponding to Oracle Internet Directory.
   - For AD, download `activedirectory-12.2.1.3.0.zip` connector bundle corresponding to Microsoft Active Directory User Management.

> **Note:**
>
> For all directory types, the required Connector version for OIG-OAM integration is 12.2.1.3.0.

2. Unzip the Connector bundle to the desired connector path under OIG Oracle home`$ORACLE_HOME/idm/server/ConnectorDefaultDirectory`.

   For example:

   ```
   /u01/app/fmw/ORACLE_HOME/idm/server/ConnectorDefaultDirectory
   ```

3. For AD, install the Active Directory User Management Connector on both, OIG and Connector server.

> **Note:**
>
> Application creation step performs the connector installation. No other install steps are necessary.

> **Important:**
>
> Post OIG-OAM integration, if the LDAP Connector bundle or the Active Directory Connector bundle is used for creating target application instances for other IT resources, then the `pre-config.xml` corresponding to the directory type must be manually imported from Sysadmin UI before proceeding to create application instance.
>
> - For OID:
>
>   ```
>   XML name: OID-pre-config.xml
>   Location (example): $ORACLE_HOME/idm/server/ConnectorDefaultDirectory/
>   OID-12.2.1.3.0/xml/OID-pre-config.xml
>   ```
>
> - For OUD/ODSEE/LDAPV3:
>
>   ```
>   XML name: ODSEE-OUD-LDAPV3-pre-config.xml
>   Location (example): $ORACLE_HOME/idm/server/ConnectorDefaultDirectory/
>   OID-12.2.1.3.0/xml/ODSEE-OUD-LDAPV3-pre-config.xml
>   ```
>
> - For AD:
>
>   ```
>   XML name: ad-pre-config.xml
>   Location (example): $ORACLE_HOME/idm/server/ConnectorDefaultDirectory/
>   activedirectory-12.2.1.3.0/xml//ad-pre-config.xml
>   ```
>
> For importing `pre-config.xml` , see Importing Connector XML File.

Assigning Lockout Threshold in LDAP Directory and Oracle Access Manager

The value for maximum number of authentication failures that a user is allowed to attempt before the user's account gets locked, should be the same in the LDAP directory and Oracle Access Manager.

To set the account lockout duration, open the `oam-config.xml` in the OAM Domain under `DOMAIN_HOME/config/fmwconfig` and update the `LockoutAttempts` parameter. To do so, export and import the `oam-config.xml` file by following the steps in Exporting and Importing the OAM Configuration File.

> **See Also:**
>
> - OID-Managing Password Policies in *Administering Oracle Internet Directory*.
> - OUD-Managing Password Policies in *Administering Oracle Unified Directory*.
> - AD-Configuring Account Lockout Policies in *Windows 2000 Evaluated Configuration Administrators Guide*.

3.3.2 Step-by-step Procedure for OIG-OAM Integration Using Automated Script

The automated integration script, `OIGOAMIntegration.sh` supports individual execution of OIG-OAM configuration operations.

> **Note:**
>
> You must run the `OIGOAMIntegration.sh` command only on the OIG server.

Prerequisites

- Installed all the components listed Prerequisites.

Perform step-by-step configuration of the OIG-OAM integrated environment by executing each integration task separately. At the end of each step, verify the log output and confirm that the configuration operation is completed successfully. If the configuration operation fails, apply appropriate fixes and rerun the step before proceeding to the next step in the integration sequence.

Run `OIGOAMIntegration.sh`, a top-level automated integration script to perform the following operations required for OIG-OAM integration:

- Populating OHS Rules
- Configuring WLS Authenticator providers
- Configuring LDAP Connector
- Configuring OIG SSO Integration
- Enabling OAM Notifications
- Restarting Servers

3.3.2.1 Populating OHS Rules Using Automated Script

Populate OHS rules using the `OIGOAMIntegration.sh` automated script.

To populate OHS rules:

1. Update the `populateOHSRedirectIdmConf.config` file (Located at `ORACLE_HOME/idm/server/ssointg/config`) with the OAM and OIG server details.

   ```
   OIM_HOST
   OIM_PORT
   OAM_HOST
   OAM_PORT
   ```

   The following table provides descriptions of the parameters in the `populateOHSRedirectIdmConf.config` file.

   Table 3-3 Parameters in `populateOHSRedirectIdmConf.config` file

Property	Description	Sample Value
`OAM_HOST`	Enter the URL for OAM server.	`oamhost.example.com`
`OAM_PORT`	Enter the port for OAM Server	`14100`
`OIM_HOST`	Enter the host name for OIG managed server.	`oimhost.example.com`
`OIM_PORT`	Enter the port for OIG Server.	`14000`

2. Run the `OIGOAMIntegration.sh` script from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/bin`) to populate OHS Rules.

   ```
   OIGOAMIntegration.sh -populateOHSRules
   ```

3. Verify that the `oim.conf` file is generated at `ORACLE_HOME/idm/server/ssointg/templates`.
4. Remove the following parameters in the `oim.conf` file.
   - `/Nexaweb`
   - `/xlWebApp`
5. Copy the `oim.conf` file from the OIG home directory (Located at `ORACLE_HOME/idm/server/ssointg/config`) to `OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf`.
6. Restart OHS Server.

   For information about restarting the Oracle HTTP Server instance, see Restarting Oracle HTTP Server Instances in *Administering Oracle HTTP Server*.

3.3.2.2 Configuring WLS Authentication Providers Using Automated Script

Configure WLS Authentication Providers using the `OIGOAMIntegration.sh` automated script for OIG-OAM integration.

You must configure the WLS Authentication Providers to set SSO logout for and security providers in OIG domain. So that both the SSO login and OIM client-based login, work appropriately.

For example, after executing `OIGOAMIntegration.sh -configureWLSAuthnProviders` script, the authenticators order would be as follows:

1. OAMIDAsserter
2. OIMSignatureAuthenticator
3. OIMAuthenticationProvider
4. LDAPAuthenticator

   Depending on the LDAP directory you are using:

   - OID: OIDAuthenticator
   - OUD: OUDAuthenticator
   - AD: ADAuthenticator
5. DefaultAuthenticator
6. DefaultIdentityAsserter
7. Trust Service Identity Asserter

To configure WLS Authentication Providers using automated script:

1. Open the `configureWLSAuthnProviders.config` file from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/config`) in a text editor and update the parameters.

   Example `configureWLSAuthnProviders.config` File

   ```
   OIM_WLSHOST: oimadminhost.example.com
   OIM_WLSPORT: 7001
   OIM_WLSADMIN: weblogic
   OIM_WLSADMIN_PWD: <password>
   OIM_SERVER_NAME: oim_server1
   IDSTORE_DIRECTORYTYPE: OID
   IDSTORE_HOST: idstore.example.com
   IDSTORE_PORT: 3060
   IDSTORE_BINDDN: cn=orcladmin
   IDSTORE_BINDDN_PWD: <password>
   IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
   IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
   ```

   The following table describes the parameters that you can set in the `configureWLSAuthnProviders.config` file.

Table 3-4 Parameters in `configureWLSAuthnProviders.config` file

Property	Description	Sample Value
`OIM_WLSHOST`	Enter the OIG admin server host name.	`oimadminhost.example.com`
`OIM_WLSPORT`	Enter the OIG admin server port.	`17001`
`OIM_WLSADMIN`	Enter the weblogic administrator user in OIM domain.	`weblogic`
`OIM_WLSADMIN_PWD`	Enter the password for the weblogic admin user in OIM domain. **Note:** All password fields are optional. If you do not enter them in the file (security issues), then you are prompted to enter them when the script runs.	`password`
`OIM_SERVER_NAME`	Enter the OIG server name.	`oim_server1`
`IDSTORE_DIRECTORYTYPE`	Enter the identity store directory type. Valid options are OID, OUD, and AD.	`OID`
`IDSTORE_HOST`	Enter the identity store host name.	`idstore.example.com`
`IDSTORE_PORT`	Enter the identity store port.	`3060`
`IDSTORE_BINDDN`	An administrative user in Oracle Internet Directory, Oracle Unified Directory or Microsoft Active Directory.	• OID: `cn=orcladmin` • OUD: `cn=oudadmin` • AD: `CN=Administrator,CN=Users,DC=example.com,DC=example,dc=com`
`IDSTORE_BINDDN_PWD`	Enter the Password for administrative user in Oracle Internet Directory, Oracle Unified Directory, or Microsoft Active Directory. **Note:** All password fields are optional. If you do not enter them in the file (security issues), then you are prompted to enter them when the script runs.	*password*
`IDSTORE_USERSEARCHBASE`	Enter the location in the directory where users are stored.	`cn=users,dc=example,dc=com`
`IDSTORE_GROUPSEARCHBASE`	Enter the location in the directory where groups are stored.	`cn=groups,dc=example,dc=com`

2. Run the `OIGOAMIntegration.sh` script from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/bin`) to configure WLS Authentication Providers:

   ```
   OIGOAMIntegration.sh -configureWLSAuthnProviders
   ```

   You have successfully executed the automated script for configuring WLS Authentication Providers.

3. Restart OIG domain servers. See Starting the Servers in *Installing and Configuring Oracle Identity and Access Management*.

3.3.2.3 Configuring LDAP Connector Using Automated Script

Configure LDAP Connector using automated script for integration, `OIGOAMIntegration.sh`.

The automated script executes the following operations and configures the LDAP Connector:

1. Copying the Application On-boarding LDAP templates into the downloaded Connector bundle.
2. Obtaining application names and other property values such as LDAP host and port from the configuration file.
3. Creating Application objects, target application and authoritative application, from the unmarshalled LDAP templates.
4. Executing `create` API method through the Application Manager to create the Application Instances from the Application objects.
5. Updating the IT Resource instance with values obtained from the configuration file as follows:
   - baseContexts
   - principal
   - credentials
   - host and port
   - SSL (`true` or `false`)
6. Setting `SSO.DefaultCommonNamePolicyImpl` system property.
7. Setting properties in `SSOIntegrationMXBean` with values obtained from the configuration file:
   - `targetAppInstanceName`
   - `targeITResourceNameForGroup`
   - `directorytype`
8. Updating the scheduled jobs with the SSO trusted and target parameters.
9. Updating container rules by invoking SSOIntegrationMXBean `addContainerRules` operation with values obtained from the configuration file:
   - Directory type
   - User search base

- User search base description
- Group search base
- Group search base description

> **Note:**
>
> Executing the script for configuring connector seeds only the default LDAP container rules into MDS. You can use custom container rules and manually upload them to MDS.

To configure the LDAP Connector:

1. Open the `configureLDAPConnector.config` file from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/config`) in a text editor and update the parameters.

   Example `configureLDAPConnector.config` File

```
IDSTORE_DIRECTORYTYPE=OID
OIM_HOST=oimhost.example.com
OIM_PORT=14000
WLS_OIM_SYSADMIN_USER=<system_administrator_username>
WLS_OIM_SYSADMIN_USER_PWD=<password>
OIM_WLSHOST=oimadminhost.example.com
OIM_WLSPORT=7001
OIM_WLSADMIN=weblogic
OIM_WLSADMIN_PWD=<password>
OIM_SERVER_NAME=oim_server1
IDSTORE_HOST=idstore.example.com
IDSTORE_PORT=3060
IDSTORE_BINDDN=cn=orcladmin
IDSTORE_BINDDN_PWD=<password>
IDSTORE_OIMADMINUSERDN=cn=oimLDAP,cn=systemids,dc=example,dc=com
IDSTORE_OIMADMINUSER_PWD=<password>
IDSTORE_SEARCHBASE=dc=example,dc=com
IDSTORE_USERSEARCHBASE=cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE=cn=Groups,dc=example,dc=com
IDSTORE_USERSEARCHBASE_DESCRIPTION=Default user container
IDSTORE_GROUPSEARCHBASE_DESCRIPTION=Default group container
IDSTORE_EMAIL_DOMAIN=example.com
## For ActiveDirectory use the values of "yes" or "no". i.e.
IS_LDAP_SECURE=yes/no
IS_LDAP_SECURE=false
SSO_TARGET_APPINSTANCE_NAME=SSOTarget
## Path to expanded connector bundle: e.g. for OID and OUD
CONNECTOR_MEDIA_PATH=/u01/oracle/products/identity/idm/server/
ConnectorDefaultDirectory/OID-12.2.1.3.0
## Path for AD bundle
# CONNECTOR_MEDIA_PATH=/u01/oracle/products/identity/idm/server/
ConnectorDefaultDirectory/activedirectory-12.2.1.3.0
## [ActiveDirectory]
# The following attributes need to be initialized only if Active
Directory is the target server
```

```
# AD_DIRECTORY_ADMIN_NAME=oimLDAP@example.com
# AD_DIRECTORY_ADMIN_PWD=<password>
# AD_DOMAIN_NAME=example.com
## Active Directory Connector Server details
# AD_CONNECTORSERVER_HOST=192.168.99.100
# AD_CONNECTORSERVER_KEY=<connectorserverkey>
# AD_CONNECTORSERVER_PORT=8759
# AD_CONNECTORSERVER_TIMEOUT=0
## Set to yes if SSL is enabled
# AD_CONNECTORSERVER_USESSL=no
```

The following table describes the parameters that you can set in the in the `configureLDAPConnector.config` file.

Table 3-5 Parameters in `configureLDAPConnector.config` file

Property	Description	Sample Value
`IDSTORE_DIRECTORYTYPE`	Enter the identity store directory type. Valid options are OID, OUD, and AD.	`OID`
`OIM_HOST`	Enter the host name for OIG managed server.	`oimhost.example.com`
`OIM_PORT`	Enter the port for OIG Server.	`14000`
`WLS_OIM_SYSADMIN_USER`	Enter the system admin user to be used to connect to OIG while configuring SSO. This user needs to have system admin role.	`xelsysadm`
`WLS_OIM_SYSADMIN_USER_PWD`	Enter the password for OIG system administrator user. **Note:** All password fields are optional. If you do not enter them in the file (security issues), then you are prompted to enter them when the script runs.	*`password`*
`OIM_WLSHOST`	Enter the OIG admin server host name.	`oimadminhost.example.com`
`OIM_WLSPORT`	Enter the OIG admin server port.	`17001`
`OIM_WLSADMIN`	Enter the weblogic administrator user in OIM domain.	`weblogic`

Table 3-5 (Cont.) Parameters in `configureLDAPConnector.config` file

Property	Description	Sample Value
`OIM_WLSADMIN_PWD`	Enter the password for the weblogic admin user in OIM domain. **Note:** All password fields are optional. If you do not enter them in the file (security issues), then you are prompted to enter them when the script runs.	*password*
`OIM_SERVER_NAME`	Enter the OIG server name. **Note:** You must manually add the `OIM_SERVER_NAME` property in the `configureLDAPConnector.config` file.	`oim_server1`
`IDSTORE_HOST`	Enter the identity store host name.	`idstore.example.com`
`IDSTORE_PORT`	Enter the identity store port.	`3060`
`IDSTORE_BINDDN`	An administrative user in Oracle Internet Directory, Oracle Unified Directory or Active Directory.	• OID: `cn=orcladmin` • OUD: `cn=oudadmin` • AD: `CN=Administrator, CN=Users, DC=example.com, DC=example, dc=com`
`IDSTORE_BINDDN_PWD`	Enter the Password for administrative user in Oracle Internet Directory, Oracle Unified Directory, or Microsoft Active Directory.	*password*
`IDSTORE_OIMADMINUSERDN`	Enter the location of a container in the directory where system-operations users are stored. There are only a few system-operations users and are kept separate from enterprise users stored in the main user container. For example, the Oracle Identity Governance reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.	`cn=oimLDAP,cn=systemids,dc=example,dc=com`

Table 3-5 (Cont.) Parameters in `configureLDAPConnector.config` file

Property	Description	Sample Value
`IDSTORE_OIMADMINUSER_PWD`	Enter the Password for the user that Oracle Identity Governance uses to connect to the identity store.	*password*
`IDSTORE_SEARCHBASE`	Enter the location in the directory where users and groups are stored.	`dc=example,dc=com`
`IDSTORE_USERSEARCHBASE`	Enter the Container under which Access Manager searches for the users.	`cn=users,dc=example, dc=com`
`IDSTORE_GROUPSEARCHBASE`	Enter the location in the directory where groups are stored.	`cn=groups, dc=example, dc=com`
`IDSTORE_USERSEARCHBASE_DESCRIPTION`	Enter the description for the directory user search base	Default user container
`IDSTORE_GROUPSEARCHBASE_DESCRIPTION`	Enter the description for the directory group search base.	Default group container
`IDSTORE_EMAIL_DOMAIN`	Enter the domain used for e-mail For example, `user@example.com`.	`example.com`
`IS_LDAP_SECURE`	It indicates the usage of SSL for LDAP Communication. Use `yes` or `no` for ActiveDirectory.	`false`
`SSO_TARGET_APPINSTANCE_NAME`	Enter the Target application instance name used for provisioning account to target LDAP.	`SSOTarget`
`CONNECTOR_MEDIA_PATH`	Enter the location of the Connector bundle downloaded and unzipped. Oracle Identity Governance would use this location to pick the Connector bundle to be installed.	• OID/OUD: `ORACLE_HOME/idm/server/ConnectorDefaultDirectory/OID-12.2.1.3.0` • AD: `ORACLE_HOME/idm/server/ConnectorDefaultDirectory/activedirectory-12.2.1.3.0`
`AD_DIRECTORY_ADMIN_NAME`	Name of AD Admin	`oimLDAP@example`
`AD_DIRECTORY_ADMIN_PWD`	Enter the password for the AD Directory Admin.	*password*
`AD_DOMAIN_NAME`	Enter the domain name configured in Microsoft Active Directory.	`example.com`
`AD_CONNECTORSERVER_HOST`	Enter the host name or IP address of the computer hosting the connector server.	`192.0.2.1`
`AD_CONNECTORSERVER_KEY`	Enter the key for the connector server.	<connectorserverkey>

Table 3-5 (Cont.) Parameters in `configureLDAPConnector.config` file

Property	Description	Sample Value
`AD_CONNECTORSERVER_PORT`	Enter the number of the port at which the connector server is listening.	`8759`
`AD_CONNECTORSERVER_TIMEOUT`	Enter an integer value that specifies the number of milliseconds after which the connection between the connector server and the Oracle Identity Governance times out. A value of `0` means that the connection never times out.	`0`
`AD_CONNECTORSERVER_USESSL`	Enter `true` to specify that you will configure SSL between Oracle Identity Governance or Oracle Unified Directory and the Connector Server. Otherwise, enter `false`. For Active Directory, the value should be `yes` or `no`. The default value is `false` **Note:** It is recommended that you configure SSL to secure communication with the connector server.	`true` (or `false`)

2. Run the `OIGOAMIntegration.sh` script from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/bin`) to configure the LDAP Connector:

```
OIGOAMIntegration.sh -configureLDAPConnector
```

You have successfully executed the automated script for configuring LDAP Connector.

Verifying the LDAP Connector Configuration

You can verify the LDAP Connector configuration by performing the following steps:

1. Verify that the target application instances are created:
   a. Open a browser, and access the Oracle the Identity Self Service login page using the following URL format:

      `http://OIM_HOST.com:PORT/identity/`

   b. Click the **Manage** tab, and then click the **Applications** box to open the Applications page.
   c. Click the **Search** icon.

      The search results table displays the Target application instance name (The values entered in `configureLDAPConnector.config` file.) used for provisioning account to target LDAP.

      For example, **SSOTarget** and **SSOTrusted-for-SSOTarget**.

d. Select **SSOTarget**, and click **Setting**.

e. From the **User** section, select **Organization**.

f. Verify that the application is configured to be published to the Top organization.

2. Verify that the IT Resource instance is updated with the required parameters you have updated in the `configureLDAPConnector.config` file:

   a. Open a browser, and access the Oracle Identity System Administration Console using the following URL format:

      `http://HOSTNAME:PORT/sysadmin`

   b. Under Provisioning Configuration, click **IT Resource**.

      The Manage IT Resources page is displayed.

   c. Search the SSO Server IT Resources and verify that the following attributes are updated with the parameters you specified in the `configureLDAPConnector.config` file:

      - `baseContexts`
      - `principal`
      - `credentials`
      - `host and port`
      - `SSL (true or false)`

3. Verify that the **SSO.DefaultCommonNamePolicyImpl** system property is updated with the value **oracle.iam.ssointg.impl.handlers.account.commonname.plugins.impl.FirstNameLastNamePolicy** using the Oracle Identity System Administration Console.

4. Verify that the `SSOIntegrationMXBean` is updated with the required parameters you have updated in the `configureLDAPConnector.config` file:

   a. Open a browser, and access the Oracle Enterprise Manager Fusion Middleware Control for the OIG using the following URL format:

      `http://ADMINSTRATION_SERVER:PORT/em`

   b. Expand **Domain** and open **System MBean Browser**.

   c. Search the mbean with name `SSOIntegrationMXBean`.

   d. Verify that the following attributes are updated with the parameters you specified in the `configureLDAPConnector.config` file:

      - `DirectoryType`
      - `TargetAppInstanceName`
      - `TargetITResourceNameForGroup`

3.3.2.4 Configuring SSO Integration Using Automated Script

Configure SSO Integration using automated script for integration, `OIGOAMIntegration.sh`.

Use `OIGOAMIntegration.sh` to register OIM as TAP partner for OAM, add the resource policies for OIG-OAM communication, and update SSOIntegrationMXBean values in MDS.

To configure SSO integration:

1. Open the `configureSSOIntegration.config` file from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/config`) in a text editor and update the parameters.

   Example `configureSSOIntegration.config` File

```
NAP_VERSION: 4
COOKIE_EXPIRY_INTERVAL: 120
OAM_HOST: oamhost.example.com
OAM_PORT: 14100
ACCESS_SERVER_HOST: oamaccesshost.example.com
ACCESS_SERVER_PORT: 5557
OAM_SERVER_VERSION: 11g
WEBGATE_TYPE: ohsWebgate11g
ACCESS_GATE_ID: Webgate_IDM
ACCESS_GATE_PWD: <password>
COOKIE_DOMAIN: .example.com
OAM_TRANSFER_MODE: Open
SSO_ENABLED_FLAG: true
SSO_INTEGRATION_MODE: CQR
OIM_LOGINATTRIBUTE: User Login
OAM11G_IDSTORE_NAME: OAMIDSTORE
OAM11G_WLS_ADMIN_HOST: oamadminhost.example.com
OAM11G_WLS_ADMIN_PORT: 7001
OAM11G_WLS_ADMIN_USER: weblogic
OAM11G_WLS_ADMIN_PASSWD: <password>
## Required if OAM_TRANSFER_MODE is not OPEN
#SSO_KEYSTORE_JKS_PASSWORD: <password>
#SSO_GLOBAL_PASSPHRASE: <passphrase>
OIM_WLSHOST: oimadminhost.example.com
OIM_WLSPORT: 7001
OIM_WLSADMIN: weblogic
OIM_WLSADMIN_PWD: <password>
OIM_SERVER_NAME: oim_server1
IDSTORE_OAMADMINUSER: oamAdmin
IDSTORE_OAMADMINUSER_PWD: <password>
## Required in SSL mode
#OIM_TRUST_LOC=/u01/oracle/products/identity/wlserver/server/lib/
DemoTrust.jks
#OIM_TRUST_PWD=<password>
#OIM_TRUST_TYPE=JKS
```

   The following table describes the parameters that you can set in the `configureSSOIntegration.config` file.

Table 3-6 Parameters in `configureSSOIntegration.config` File

Property	Description	Sample Value
NAP_VERSION	Enter the NAP protocol version. (4 indicates 11g+)	4
OAM11G_IDSTORE_NAME	Enter the name of the identity Store configured in OAM. This will be set as the default/System ID Store in OAM.	OAMIDStore
COOKIE_EXPIRY_INTERVAL	Enter the Cookie expiration period.	120
OAM_HOST	Enter the hostname for OAM server.	oamhost.example.com
OAM_PORT	Enter the port for OAM Server	14100
ACCESS_SERVER_HOST	Enter the Access Manager OAP host.	oamaccesshost.example.com
ACCESS_SERVER_PORT	Enter the Access Manager OAP port.	5575
OAM_SERVER_VERSION	Only OAM 12c is supported. OAM 10g is not supported in 12c integration.	11g
WEBGATE_TYPE	Enter the WebGate agent type you want to create. 10g is no longer supported in 12c.	ohsWebgate12c or ohsWebgate11g
ACCESS_GATE_ID	Name to be assigned to the WebGate. This is the value specified during OAM configuration. For more information, see Configuring OAM Using Automated Script.	Webgate_IDM
ACCESS_GATE_PWD	Enter the Password for Access Gate ID.	<password>
COOKIE_DOMAIN	Enter the domain in which the WebGate functions.	.example.com
OAM_TRANSFER_MODE	Enter the security mode in which the access servers function. Supported values are OPEN and SIMPLE. Oracle recommends using SIMPLE as a minimum. **Note:** Switching the integration of CERT mode can be done as a postconfiguration step by changing OAM Server and the WebGate, which can be modified as described in Securing Communication Between OAM Servers and WebGates in *Administering Oracle Access Manager*.	SIMPLE
SSO_ENABLED_FLAG	Set it to true if OIG-OAM integration is enabled. False, otherwise.	true

Table 3-6 (Cont.) Parameters in `configureSSOIntegration.config` File

Property	Description	Sample Value
`SSO_INTEGRATION_MODE`	Enter the integration mode with OAM. With Challenge Question Response (CQR) mode, OIG will handle the password policy and password operations. With One Time Password (OTP) mode, any password operations will be handled by OAM itself and there will be no password change or reset in OIG.	`CQR`
`OIM_LOGINATTRIBUTE`	Enter the login attribute of the identity store that contains the user's login name. User uses this attribute for logging in. For example, User Login.	User Login
`OAM11G_WLS_ADMIN_HOST`	Enter the host for Admin server in OAM Domain.	`oamadminhost.example.com`
`OAM11G_WLS_ADMIN_PORT`	Enter the port for Admin server in OAM domain.	`7001`
`OAM11G_WLS_ADMIN_USER`	Enter the weblogic administrator user in OAM domain.	`weblogic`
`OAM11G_WLS_ADMIN_PASSWD`	Enter the password for the weblogic admin user in OAM domain. **Note:** All password fields are optional. If you do not enter them in the file (security issues), then you are prompted to enter them when the script runs.	*password*
`SSO_KEYSTORE_JKS_PASSWORD`	Enter the password for keystore, required for SIMPLE mode communication with OAM.	*password*
`SSO_GLOBAL_PASSPHRASE`	The random global passphrase for `SIMPLE` security mode communication with Access Manager. By default, Access Manager is configured to use the `OPEN` security mode. If you want to use the installation default of `OPEN` mode, you can skip this property. **Note:** The global passphrase is obtained from the value of the `global_passphrase` attribute in the saved connection configuration file. For information about this connection configuration file, see Saved Connection Configuration File.	*password*

Table 3-6 (Cont.) Parameters in `configureSSOIntegration.config` File

Property	Description	Sample Value
`OIM_WLSHOST`	Enter the OIG admin server host name.	`oimadminhost.example.com`
`OIM_WLSPORT`	Enter the OIG admin server port.	`17001`
`OIM_WLSADMIN`	Enter the weblogic administrator user in OIM domain.	`weblogic`
`OIM_WLSADMIN_PWD`	Enter the password for the weblogic admin user in OIM domain.	<password>
`OIM_SERVER_NAME`	Enter the OIG server name.	`oim_server1`
`IDSTORE_OAMADMINUSER`	Enter the user you use to access your Oracle Access Management Console.	`oamAdmin`
`IDSTORE_OAMADMINUSER_PWD`	Enter the password for the user you use to access your Oracle Access Management Console.	<password>
`OIM_TRUST_LOC`	Enter the location of the OIG trust store.	`ORACLE_HOME/wlserver/server/lib/DemoTrust.jks`
`OIM_TRUST_PWD`	Enter the password to access the trust store	<password>
`OIM_TRUST_TYPE`	Enter the type of the trust store. `JKS`, by default	JKS

2. Run the `OIGOAMIntegration.sh` script from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/bin`) to configure SSO Integration:

```
OIGOAMIntegration.sh -configureSSOIntegration
```

Note:

When you run the `OIMOAMIntegration.sh` script with the `configureSSOIntegration` option, a command not found error is displayed. However, this is a benign error and the script continues to run, as shown:

```
[2020-09-11 08:26:05]
-----------------------------------------------------------------
[2020-09-11 08:26:05]
[2020-09-11 08:26:05] ================================================
[2020-09-11 08:26:05] Executing configureSSOIntegration
[2020-09-11 08:26:05] ------------------------------------------------
[2020-09-11 08:26:05]
/scratch/username_folder/interopps4/oimmw/idm/server/ssointg/bin/
_OIGOAMIntegration.sh
: line 72: =OAM_IDSTORE_NAME: command not found
[2020-09-11 08:26:05] Now running wlst.sh updateOAMConfigIDStore.py

Initializing WebLogic Scripting Tool (WLST) ...

Welcome to WebLogic Server Administration Scripting Shell
```

The `OIGOAMIntegration.sh` adds the following policy to OAM:

```
/FacadeWebApp/*
/OIGUI/*
/iam/governance/*
/soa/**
/ucs/**
/reqsvc/**
/workflowservice/**
/HTTPClnt/**
/callbackResponseService/**
/role-sod/**
/sysadmin/**
/oim/**
/admin/**
/spml-xsd/**
/spmlws/**
/sodcheck/**
/SchedulerService-web/**
/jmx-config-lifecycle/**
/integration/**
/identity/**
/provisioning-callback/**
/soa-infra/**
/CertificationCallbackService/**
/identity/faces/firstlogin
/admin/faces/pages/pwdmgmt.jspx
/sysadmin/
/xmlpserver
/sysadmin
/identity/faces/taskdetails
/identity/faces/trackregistrationrequests
```

```
/identity/faces/request
/identity/
/identity
/sysadmin/faces/home
/identity/faces/home
/oim/faces/pages/Admin.jspx
/oim/faces/pages/Self.jspx
/admin/faces/pages/Admin.jspx
```

3. Add the following policies to OAM:
   a. Log in to the Oracle Access Management Console:

      `http://oam_adminserver_host:oam_adminserver_port/oamconsole`

   b. From the **Application Security** Launch Pad, click **Application Domains** in the Access Manager section.

      The Search Application Domains page is displayed.

   c. Click **Search** on the Search page.

      A list of Application domains appears.

   d. Click the domain **IAM Suite**.

   e. Click the **Resources** Tab.

   f. Click **Create**.

   g. Select **HTTP** as the Resource Type and **IAMSuiteAgent** as the Host Identifier.

   h. Enter the following Resource URLs:

      > **Note:**
      >
      > Choose the **Protection Level** as **Excluded**.

      - `/iam/governance/configmgmt/**`
      - `/iam/governance/scim/v1/**`
      - `/iam/governance/token/api/v1/**`
      - `/iam/governance/applicationmanagement/**`
      - `/iam/governance/adminservice/api/v1/**`
      - `/iam/governance/selfservice/api/v1/**`

   i. Click **Apply**.

4. Seed the OIG Policy Resources by performing the following steps:
   a. Run `wlst.sh` from `$ORACLE_HOME <OIG_INSTALL_LOCATION>/oracle_common/common/bin`

   b. Type `connect()`

   c. Provide OAM domain Admin username. For example, `weblogic`

   d. Provide OAM domain Admin password

e. Provide the OAM Admin server URL. For example, `t3://<OAM Host>:<OAM WLS Port>`

f. Run the following command:

```
importPolicyDelta(pathTempOAMPolicyFile="ORACLE_HOME
<OAM_INSTALL_LOCATION>/idm/oam/def_import_policies/oim-resource-
policy.xml",
isAppDomainUpdate="true")
```

5. Verify the attribute version in `SSOIntegrationMXBean`.

a. Open a browser, and access the Oracle Enterprise Manager Fusion Middleware Control for the OIG using the following URL format:

`http://ADMINSTRATION_SERVER:PORT/em`

b. Expand **Domain** and open **System MBean Browser**.

c. Search the mbean with name `SSOIntegrationMXBean`.

d. Click **SSOIntegrationMXBean**.

e. Make sure that the **attribute Version = 11g**.

> **Note:**
>
> Perform the above steps to enable auto-login in a new 12.2.1.4.0 integrated environment.

You have successfully executed the automated script for configuring SSO Integration.

Verifying the SSO Integration Configuration

Perform the following steps:

1. Verify the resources

a. Log in to the Oracle Access Management Console:

`http://oam_adminserver_host:oam_adminserver_port/oamconsole`

b. From the **Application Security** Launch Pad, click **Application Domains** in the Access Manager section.

The Search Application Domains page is displayed.

c. Click **Search** on the Search page.

A list of Application domains appears.

d. Click the domain **IAM Suite**.

e. Click the **Resources** tab and verify that the following resources are created.

- `/soa/**`
- `/jmx-config-lifecycle/**`
- `/SchedulerService-web/**`
- `/sodcheck/**`
- `/spmlws/**`

- /spml-xsd/**
- /XIMDD/**
- /admin/**
- /oim/**
- /sysadmin/**
- /role-sod/**
- /callbackResponseService/**
- /HTTPClnt/**
- /iam/governance/*
- /OIGUI/*
- /FacadeWebApp/*
- /provisioning-callback/**
- /CertificationCallbackService/**
- /iam/governance/configmgmt/**
- /iam/governance/scim/v1/**
- /iam/governance/token/api/v1/**
- /iam/governance/applicationmanagement/**
- /iam/governance/adminservice/api/v1/**
- /iam/governance/selfservice/api/v1/**

2. Verify that the `proposed value` in the `oig-oam-integration` log file and the values in the `SSOIntegrationMXBean` are same.

   a. Open the `oig-oam-integration` log file (Located at `ORACLE_HOME/idm/server/ssointg/logs`) and search for the `proposed value`.

   Example `oig-oam-integration` Log File

```
OIMIntegrationAutomationTool.connectToDomainRuntime...
Connecting to t3://myhost.us.example.com:7002
OIMIntegrationAutomationTool.getJMXConnector...
mserver: /jndi/weblogic.management.mbeanservers.domainruntime
Connection to domain runtime mbean server established
SSOIntegrationMXBean name:
oracle.iam:Location=oim_server1,name=SSOIntegrationMXBean,type=IA
MAppRuntimeMBean,Application=oim
sak SSOIntegrationAutomationTool: got SSOIntegrationMXBean...
 sak current value of accessServerHost=myhost.us.example.com
 proposed value of accessServerHost=myhost.us.example.com
  sak new value of accessServerHost=myhost.us.example.com
 sak current value of oamAdminUser=oamAdminUser
 sak proposed value of oamAdminUser=oamAdminUser
 sak new value of oamAdminUser=oamAdminUser
 current value of tapEndpointUrl=http://
myhost.us.example.com:14100/oam/server/dap/cred_submit
```

```
 sak proposed value of tapEndpointUrl=http://
myhost.us.example.com:14100/oam/server/dap/cred_submit
 sak new value of tapEndpointUrl=http://
myhost.us.example.com:14100/oam/server/dap/cred_submit
 current value of loginIdAttribute=User Login
 current value of version=12c
 proposed value of version=12c
 new value of version=12c
 current value of accessServerPort=5575
 proposed value of accessServerPort=5575
 new value of accessServerPort=5575
 current value of oamServerPort=14100
 proposed value of oamServerPort=14100
 new value of oamServerPort=5575
 current value of accessGateID=Webgate_IDM
 proposed value of accessGateID=Webgate_IDM
 new value of accessGateID=Webgate_IDM
 current value of napVersion=4
 proposed value of napVersion=4
 new value of napVersion=4
 current value of cookieDomain=.us.example.com
 proposed value of cookieDomain=.us.example.com
 new value of cookieDomain=.us.example.com
 current value of cookieExpiryInterval=120
 proposed value of cookieExpiryInterval=120
 new value of cookieExpiryInterval=120
 current value of transferMode=Open
 proposed value of transferMode=Open
 new value of transferMode=Open
 current value of webgateType=ohsWebgate11g
 proposed value of webgateType=ohsWebgate11g
 new value of webgateType=ohsWebgate11g
 proposed value of SSOEnabled=true
 new value of isSSOEnabled=true
 current value of integrationMode=CQR
 proposed value of integrationMode=CQR
 new value of integrationMode=CQR
 Connection closed sucessfully
 sak configure oam

 Connecting to OAM Domain MBean Server... looking for OAM domain
credentials.
 JMX URL : service:jmx:t3://myhost.us.example.com:7001/jndi/
weblogic.management.mbeanservers.domainruntime
 sak mbeanObjectNames size: 1
 sak Registering OIM as a TAP partner with OAM...
 sak Registering OIM as a TAP partner with OAM was successful!!
 sak configure oam before
strCipherKey=DEC40506366E926CACC9A0D666E94F85
 sak mbeanObjectNames size: 1
 Getting OAM/TAP Endpoint URL...
 Getting OAM/TAP Endpoint URL was successful!!
 MBean server connection closed sucessfully
```

b. Open a browser, and access the Oracle Enterprise Manager Fusion Middleware Control for the OIG using the following URL format:

   `http://ADMINSTRATION_SERVER:PORT/em`

c. Expand **Domain** and open **System MBean Browser**.

d. Search the mbean with name `SSOIntegrationMXBean`.

e. Ensure that all the required fields are updated as per the `proposed value` in the `oig-oam-integration` log file.

3. Open the `oam-config.xml` in the OAM Domain under `DOMAIN_HOME/config/fmwconfig` and verify that `UserStore` attribute points to the name of the identity store you specified in the `configureSSOIntegration.config` file (For example, `OAMIDSTORE`).

3.3.2.5 Enabling OAM Notifications Using Automated Script

Enable OAM notifications using the `OIGOAMIntegration.sh` automated script for OIG-OAM integration.

Event handlers are required to terminate user sessions. OAM notification handlers are not loaded by default. Run `OIGOAMIntegration.sh -enableOAMsessionDeletion` to import OAM notification handlers and register OIG System Administrator to utilize OAM REST APIs.

To enable OAM notification:

1. Open the `enableOAMSessionDeletion.config` file from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/config`) in a text editor and update the parameters.

   Example `enableOAMSessionDeletion.config` File

```
OIM_WLSHOST: oimadminhost.example.com
OIM_WLSPORT: 7001
OIM_WLSADMIN: weblogic
OIM_WLSADMIN_PWD: <password>
OIM_SERVER_NAME: oim_server1
IDSTORE_DIRECTORYTYPE: OID
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 3060
## Specify the IDStore admin credentials below
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_BINDDN_PWD: <password>
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_OAMADMINUSER: oamAdmin
IDSTORE_OAMSOFTWAREUSER: oamLDAP
```

   The following table describes the parameters that you can set in the `enableOAMSessionDeletion.config` file.

Table 3-7 Parameters in `enableOAMSessionDeletion.config` File

Property	Description	Sample Value
`OIM_WLSHOST`	Enter the OIG admin server host name.	`oimadminhost.example.com`
`OIM_WLSPORT`	Enter the OIG admin server port.	`17001`
`OIM_WLSADMIN`	Enter the weblogic administrator user in OIM domain.	`weblogic`
`OIM_WLSADMIN_PWD`	Enter the password for the weblogic admin user in OIM domain.	`password`
`OIM_SERVER_NAME`	Enter the OIG server name. **Note:** You must manually add the `OIM_SERVER_NAME` property in the `enableOAMSessionDeletion.config` file.	`oim_server1`
`IDSTORE_DIRECTORYTYPE`	Enter the identity store directory type. Valid options are OID, OUD, and AD.	`OID`
`IDSTORE_HOST`	Enter the identity store host name.	`idstore.example.com`
`IDSTORE_PORT`	Enter the identity store port.	`3060`
`IDSTORE_BINDDN`	An administrative user in Oracle Internet Directory, Oracle Unified Directory or Active Directory.	• OID: `cn=orcladmin` • OUD: `cn=oudadmin` • AD: `CN=Administrator,CN=Users,DC=example.com,DC=example,dc=com`
`IDSTORE_BINDDN_PWD`	Enter the Password for administrative user in Oracle Internet Directory, Oracle Unified Directory or Microsoft Active Directory.	*password*
`IDSTORE_USERSEARCHBASE`	Enter the location in the directory where users are stored.	`cn=users,dc=example,dc=com`
`IDSTORE_GROUPSEARCHBASE`	Enter the location in the directory where groups are stored.	`cn=groups,dc=example,dc=com`
`IDSTORE_SYSTEMIDBASE`	Enter the location of a container in the directory where system-operations users are stored. There are only a few system operations users and are kept separate from enterprise users stored in the main user container. For example, the Oracle Identity Governance reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.	`cn=systemids,dc=example,dc=com`
`IDSTORE_OAMADMINUSER`	Enter the user you use to access your Oracle Access Management Console.	`oamAdmin`

Table 3-7 (Cont.) Parameters in `enableOAMSessionDeletion.config` File

Property	Description	Sample Value
`IDSTORE_OAMSOFTWAREUSER`	Enter the user you use to interact with the LDAP server.	`oamLDAP`

> **Note:**
>
> You must manually add the WebLogicCluster parameter to the list of Managed Servers in the cluster:

2. Run the `OIGOAMIntegration.sh` script from the OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/bin`) to enable OAM notifications:

```
OIGOAMIntegration.sh -enableOAMSessionDeletion
```

You have successfully executed the automated script to enable OAM notifications.

3. To verify the configuration, navigate to OIG MDS and ensure that the following event handlers exist under `/db/ssointg/`:
   - `EventHandlers.xml`
   - `ldapconnector_sso_eventhandlers.xml`

3.3.2.6 Restarting Servers

After executing the automated script to complete the OIG-OAM integration process, restart all the servers.

1. Before restarting the servers, OAM requires access to MBeans stored within the administration server. In order for LDAP users to be able to log in to the WebLogic console and Fusion Middleware control, they must be assigned the WebLogic Administration rights. In order for OAM to invoke these Mbeans, users in the OAMAdministrators group must have WebLogic Administration rights. To add the LDAP Groups `OAMAdministrators` and `WLSAdministrators` to the WebLogic Administrators:
   a. Log in to the WebLogic Administration Server Console as the default administrative user. For example, `weblogic`.
   b. In the left pane of the console, click **Security Realms**.
   c. On the Summary of Security Realms page, click **myrealm** under the Realms table.
   d. On the Settings page for **myrealm**, click the **Roles & Policies** tab.
   e. On the Realm Roles page, expand the **Global Roles** entry under the Roles table.
   f. Click the **Roles** link to go to the Global Roles page.
   g. On the Global Roles page, click the **Admin** role to go to the Edit Global Roles page.

h. On the Edit Global Roles page, under the **Role Conditions** table, click the **Add Conditions** button.

i. On the Choose a Predicate page, select **Group** from the drop down list for predicates and click **Next**.

j. On the Edit Arguments Page, Specify **OAMAdministrators** in the **Group Argument** field and click **Add**.

k. Repeat for the Group **WLSAdministrators**.

l. Click **Finish** to return to the Edit Global Roles page.

m. The **Role Conditions** table now shows the groups **OAMAdministrators or WLSAdministrators** as role conditions.

n. Click **Save** to finish adding the Admin role to the OAMAdministrators and IDM Administrators Groups.

2. Restart OHS Server. For information, see Restarting Oracle HTTP Server Instances in *Administering Oracle HTTP Server*.

3. Restart the OAM domain. For more information, see Starting the Servers in *Installing and Configuring Oracle Identity and Access Management*.

4. Restart OIG domain. For more information, see Starting the Serversin *Installing and Configuring Oracle Identity and Access Management*.

You have successfully executed the automated script and completed the OIG-OAM Integration process.

Proceed with validation of your integration setup. See Validating OIG-OAM integration.

3.4 Validating the Access Manager and Oracle Identity Governance Integration

Performing the following sanity checks (validating the integrated environment) can help you avoid some common issues that could be encountered during runtime.

In this release, Oracle Identity Governance is integrated with Access Manager using the `OIGOAMIntegration.sh` script. After Oracle Identity Governance is integrated with Oracle Access Manager, the following configuration settings and files are updated:

- The `SSOConfig` section in the `oim-config.xml` file, stored in the OIG Metadata store.
- The realm security providers in *`OIM_DOMAIN_HOME`*`/config.xml`.
- The OIG domain credential store in *`OIM_DOMAIN_HOME`*`/config/fmwconfig/cwallet.sso`.
- The orchestration event-handlers required for SSO integration in `Eventhandler.xml`, stored in the OIG Metadata store..
- The SSO logout configuration in *`OIM_DOMAIN_HOME`*`/config/fmwconfig/jps-config.xml`.

> **See Also:**
>
> - Validating the Oracle Identity Manager SSO Configuration Settings
> - Validating the Oracle Identity Governance Security Provider Configuration
> - Validating the Access Manager Security Provider Configuration
> - Validating the Oracle Identity Governance Event Handlers Configured for SSO
> - Validating the Oracle Identity Governance SSO Logout Configuration
> - Functionally Testing the Access Manager and Oracle Identity Governance Integration
> - Validating Integration Configuration

3.4.1 Validating the Oracle Identity Governance SSO Configuration Settings

This procedure explains how to validate the `SSOConfig` settings in `oim-config.xml`:

> **See Also:**
>
> Getting Started Using the Fusion Middleware Control MBean Browsers in *Administering Oracle Fusion Middleware*.

1. Log in to Oracle Enterprise Manager Fusion Middleware Control.
2. Select **Weblogic Domain**, then right-click the domain name.
3. Open System Mbean Browser and search for the `SSOIntegrationMXBean`.
4. Verify the following attribute settings are correct after running `OIGOAMIntegration.sh`. Update any values as needed:
   - Port of OAM Managed Server, `oamServerPort` is updated.
   - Admin user for OAM, `oamAdminUser` is updated.
   - `SsoEnabled` attribute is write-only. To ensure it is set to `true`, manually set it in the Mbean Browser.

     To check the attribute value:

     a. Open the **Operations** tab and select the `isSsoEnabled` attribute.

     b. Click the **Invoke** button to see the current value.
   - If using TAP communication, the `TapEndpointURL` attribute is present.
   - If using Oracle Access Protocol (OAP) communication, the following attributes are present: `AccessGateID`, `AccessServerHost`, `AccessServerPort`, `CookieDomain`, `CookieExpiryInterval`, `NapVersion`, `TransferMode`, `WebgateType`.

- If `Version` is set to `11g`, verify the `TapEndpointURL` attribute is set to a valid URL.
- `IntegrationMode` is set to `CQR`.
- `DirectoryType` is set to `OID` or `OUD` or `AD`.
- `TargetITResourceNameForGroup` is set to `SSO Server`
- `TargetApplicationInstanceName` is set to the application instance name used during `OIGOAMIntegration.sh` execution.

3.4.2 Validating the Oracle Identity Governance Security Provider Configuration

This procedure explains how to validate the Oracle Identity Governance Security Provider configuration.

1. In the WebLogic Server Administration Console, navigate to the **OIG domain**.
2. Navigate to **Security Realms** > **myrealm** and then click the **Providers** tab.
3. Confirm the Authentication Providers are configured as follows.

Authentication Provider	Control Flag
OAMIDAsserter	REQUIRED
OIMSignatureAuthenticator	SUFFICIENT
OIMAuthenticationProvider	SUFFICIENT
LDAP Authenticator	SUFFICIENT
DefaultAuthenticator	SUFFICIENT
DefaultIdentityAsserter	Not Applicable
Trust Service Identity Asserter	Not Applicable

4. The LDAP Authenticator name may vary depending on which LDAP provider you are using. For example for Oracle Unified Directory, it is OUDAuthenticator. Verify it is configured correctly by selecting **Users and Groups** tab, and confirming the LDAP users are listed in **Users** tab.

3.4.3 Validating the Access Manager Security Provider Configuration

This procedure explains how to validate the Access Manager Security Provider configuration.

1. In the WebLogic Server Administration Console, navigate to the **OAM domain**.
2. Navigate to **Security Realms** > **myrealm**. Then, click the **Providers** tab.
3. Confirm the Authentication Providers are configured as follows.

Authentication Provider	Control Flag
Trust Service Identity Asserter	Not applicable
OAMIDAsserter	Required
DefaultAuthenticator	SUFFICIENT
LDAP Authenticator	SUFFICIENT
DefaultIdentityAsserter	Not applicable

4. The LDAP authenticator varies depending upon the LDAP provider being used. Verify that it is configured correctly by clicking the **Users and Groups** tab, and confirming that the LDAP users are listed in **Users** tab.

3.4.4 Validating the Oracle Identity Governance Domain Credential Store

All passwords and credentials used during communication between Oracle Identity Governance and Access Manager are stored in the domain credential store.

To validate the passwords and credentials used to communicate:

1. Login to Oracle Enterprise Manager Fusion Middleware Control for the OIG domain and select **WebLogic Domain**.
2. From the **Weblogic Domain** drop-down, navigate to **Security** and click **Credentials**.
3. Expand the **oim** instance. Verify the following credentials:
   - **SSOAccessKey**: For `OPEN` mode only
   - **SSOKeystoreKey**: For `SIMPLE` mode only
   - **SSOGobalPP**: For `SIMPLE` mode only
   - **OIM_TAP_PARTNER_KEY**
   - **OAMAdminPassword**

3.4.5 Validating the Oracle Identity Governance Event Handlers Configured for SSO

A set of event handlers is uploaded to the Oracle Identity Governance MDS in order to support session termination after a user status change. These event handlers notify Access Manager when a user status is changed, which then terminates the user session. They are uploaded to MDS as part of `EventHandlers.xml` file, located at `/db/ssointg/EventHandlers.xml`.

> **See Also:**
>
> - Getting Started Using the Fusion Middleware Control MBean Browsers in *Administering Oracle Fusion Middleware*.
> - Deploying and Undeploying Customizations in *Developing and Customizing Applications for Oracle Identity Governance*.

To confirm all event handlers are configured correctly, export the `EventHandlers.xml` file using Oracle Enterprise Manager Fusion Middleware Control:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control for the OIG domain.
2. Click the **Target Navigation** icon on the left, expand **Identity and Access** then expand **Access** and click **OIM**.

3. Right-click and navigate to **System MBean Browser**.
4. Under **Application Defined MBeans**, expand each of the following: **Oracle.mds.lcm**, **Server:oim_server1**, **Application:OIM**, **MDSAppRuntime**, and click **MDSAppRuntime**.
5. Click the **Operations** tab, and then, click **exportMetadata**.
6. In **toLocation**, enter `/tmp` or the name of another directory. This is the directory where the file will be exported.
7. In the **docs** field, click **Edit** and then **Add** and enter the complete file location as the Element:

   ```
   /db/oim-config.xml
   /db/ssointg/EventHandlers.xml
   /db/LDAPContainerRules.xml
   ```

8. Select **false** for **excludeAllCust**, **excludeBaseDocs**, and **excludeExtendedMetadata**.
9. Click **Invoke** to export the files specified in the **docs** field to the directory specified in the **toLocation** field.
10. Verify list of handlers in `EventHandlers.xml`:

    ```
    <postprocess-handler
    class="oracle.iam.sso.eventhandlers.UserLockedNotificationHandler" entity-
    type="User" operation="LOCK" name="UserLockedNotificationHandler" order="FIRST"
    stage="postprocess" sync="TRUE"/>
    <postprocess-handler
    class="oracle.iam.sso.eventhandlers.UserLockedNotificationHandler" entity-
    type="User" operation="UNLOCK" name="UserLockedNotificationHandler" order="FIRST"
    stage="postprocess" sync="TRUE"/>
    <postprocess-handler
    class="oracle.iam.sso.eventhandlers.UserStatusNotificationHandler" entity-
    type="User" operation="ENABLE" name="UserStatusNotificationHandler" order="FIRST"
    stage="postprocess" sync="TRUE"/>
    <postprocess-handler
    class="oracle.iam.sso.eventhandlers.UserStatusNotificationHandler" entity-
    type="User" operation="DISABLE" name="UserStatusNotificationHandler" order="FIRST"
    stage="postprocess" sync="TRUE"/>
    <postprocess-handler
    class="oracle.iam.sso.eventhandlers.UserUpdatedNotificationHandler" entity-
    type="User" operation="MODIFY" name="UserUpdatedNotificationHandler" order="FIRST"
    stage="postprocess" sync="TRUE"/>
    <postprocess-handler
    class="oracle.iam.sso.eventhandlers.UserUpdatedNotificationHandler" entity-
    type="User" operation="DELETE" name="UserUpdatedNotificationHandler" order="FIRST"
    stage="postprocess" sync="TRUE"/>
    <action-handler class="oracle.iam.sso.eventhandlers.RoleGrantNotificationHandler"
    entity-type="RoleUser" operation="CREATE" name="RoleGrantNotification"
    order="FIRST" stage="postprocess" sync="TRUE"/>
    <action-handler class="oracle.iam.sso.eventhandlers.RoleGrantNotificationHandler"
    entity-type="RoleUser" operation="MODIFY" name="RoleGrantNotification"
    order="FIRST" stage="postprocess" sync="TRUE"/>
    <action-handler class="oracle.iam.sso.eventhandlers.RoleGrantNotificationHandler"
    entity-type="RoleUser" operation="DELETE" name="RoleGrantNotification"
    order="FIRST" stage="postprocess" sync="TRUE"/>
    ```

3.4.6 Validating the Oracle Identity Governance SSO Logout Configuration

Oracle Identity Governance logout is configured to use single logout after the integration is complete. After a user logs out from Oracle Identity Governance, they are logged out from all the Access Manager protected applications as well.

To verify the configuration of single logout, do the following:

1. From your present working directory, move to the following directory:

   OIM_DOMAIN_HOME/config/fmwconfig

2. Open the `jps-config.xml` file.

3. Ensure the `<propertySet name="props.auth.uri.0">` element in the `jps-config.xml` file contains entries similar to the following example:

```
<propertySet name="props.auth.uri.0">
<property name="logout.url" value="/oamsso/logout.html"/>
<property name="autologin.url" value="/obrar.cgi"/>
<property name="login.url.BASIC" value="/${app.context}/adfAuthentication"/>
<property name="login.url.FORM" value="/${app.context}/adfAuthentication"/>
<property name="login.url.ANONYMOUS" value="/${app.context}/
adfAuthentication"/>
</propertySet>
```

3.4.7 Functionally Testing the Access Manager and Oracle Identity Governance Integration

The final task is to verify the Access Manager and Oracle Identity Governance integration.

Perform the steps shown in the following table in sequence.

Table 3-8 Verifying Access Manager and Oracle Identity Governance Integration

Step	Description	Expected Result
1	Log in to the Oracle Access Management Console as the `weblogic_idm` user using the URL: `http://admin_server_host:admin_server_port/oamconsole`	Provides access to the administration console.

Table 3-8 (Cont.) Verifying Access Manager and Oracle Identity Governance Integration

Step	Description	Expected Result

2	Access the Oracle Identity Governance administration page with the URL:
	• For Oracle Identity Self Service:
	`http://hostname:port/identity`
	• For Oracle Identity System Administration:
	`http://hostname:port/sysadmin`
	where *hostname:port* can be for either Oracle Identity Management or OHS, depending on whether a Domain Agent or WebGate is used.
		The Oracle Access Management login page from the Access Manager managed server should display.
		Verify the links for "Forgot Password", "Register New Account" and "Track User Registration" features appear in the login page. Verify that each link works. For more information about these features, see About Password Management Scenarios.

3	Log in as `xelsysadm` (Oracle Identity Governance administrator).	The Oracle Identity Governance Admin Page should be accessible.
4	Create a new user using Oracle Identity Self Service. Close the browser and try accessing the OIG Identity Page. When prompted for login, provide valid credentials for the newly-created user.	You should be redirected to Oracle Identity Governance and be required to reset the password. After resetting the password and setting the challenge question, user should be automatically logged into the application. Auto-login should work.
5	Close the browser and access Oracle Identity Self Service.	The Oracle Access Management login page from the Access Manager managed server should display. Verify the links for "Forgot Password", "Register New Account" and "Track User Registration" features appear in the login page. Verify that each link works. For more information about these features, see About Password Management Scenarios.
6	Verify the lock/disable feature works by opening a browser and logging in as a test user. In another browser session, log in as an administrator, then lock or disable the test user account.	The user must be redirected back to the login page while accessing any of the links.
7	Verify the SSO logout feature works by logging into Oracle Identity Self Service as test user or system administrator.	Upon logout from the page, you are redirected to the SSO logout page.

3.4.8 Validating Integration Configuration

Validate that the `oam-config.xml` in the OAM Domain under `DOMAIN_HOME/config/fmwconfig` contains the IDStore provided during OAM configuration, say `OAMIDSTORE`. XML node **SessionRuntime>UserStore** should not have `UserIdentityStore1`, but `OAMIDSTORE`.

- Validate if scheduled jobs exist:
  - SSO Group Create And Update Full Reconciliation
  - SSO Group Create And Update Incremental Reconciliation
  - SSO Group Delete Full Reconciliation

  - SSO Group Delete Incremental Reconciliation
  - SSO Group Hierarchy Sync Full Reconciliation
  - SSO Group Hierarchy Sync Incremental Reconciliation
  - SSO Group Membership Full Reconciliation
  - SSO Group Membership Incremental Reconciliation
  - SSO Post Enable Provision Role Hierarchy to LDAP
  - SSO Post Enable Provision Roles to LDAP
  - SSO Post Enable Provision Users to LDAP
  - SSO User Incremental Reconciliation
  - SSO User Full Reconciliation
  - SSO Post Enable Provision Role Membership to LDAP
- Validate if the IT Resources are updated or created appropriately.
  - Navigate to Provisioning **Configuration>ITResource**.
  - Search for IT resource Type **OID Connector**.
  - Verify that IT Resources such as `SSOTargetApp` and `SSOTrusted-for-SSOTargetApp` have correct parameter values.
- Verify that the log at `$ORACLE_HOME/idm/server/ssointg/logs/oig-oam-integration_*.log` contains:

```
[2017-12-22 02:25:13] Seeding OIM Resource Policies into OAM
[2017-12-22 02:25:13] Loading xml... /scratch/userid/devtools/
Middleware///idm/server/ssointg/templates/Resources.xml
[2017-12-22 02:25:14] Loading xml... /scratch/userid/devtools/
Middleware///idm/server/ssointg/templates/AuthnPolicies.xml
[2017-12-22 02:25:14] Loading xml... /scratch/userid/devtools/
Middleware///idm/server/ssointg/templates/AuthzPolicies.xml
[2017-12-22 02:25:14] Getting Application Domains...
[2017-12-22 02:25:14] WebResourceClient::getAppDomainResource(): http://
host:port/oam/services/rest/11.1.2.0.0/ssa/policyadmin/appdomain
[2017-12-22 02:25:15] Authenticating using {oamAdmin:******}
[2017-12-22 02:25:15] Getting Resources from domain 'IAM Suite'
[2017-12-22 02:25:15] WebResourceClient::getResource(): http://host:port/oam/
services/rest/11.1.2.0.0/ssa/policyadmin/resource
[2017-12-22 02:25:16] Getting Resources from domain 'Fusion Apps Integration'
[2017-12-22 02:25:16] WebResourceClient::getResource(): http://host:port/oam/
services/rest/11.1.2.0.0/ssa/policyadmin/resource
[2017-12-22 02:25:16] Getting Authentication Policies from domain 'IAM Suite'
[2017-12-22 02:25:16] WebResourceClient::getAuthenticationPolicyResource():
http://host:port/oam/services/rest/11.1.2.0.0/ssa/policyadmin/authnpolicy
[2017-12-22 02:25:16] Getting Authorization Policies from domain 'IAM Suite'
[2017-12-22 02:25:16] WebResourceClient::getAuthorizationPolicyResource():
http://host:port/oam/services/rest/11.1.2.0.0/ssa/policyadmin/authzpolicy
[2017-12-22 02:25:16] Resources Seeded!!
```

3.4.9 Improving Reset Password Performance in Active Directory Integration

To improve the performance of Reset Password operation in Active Directory (AD) integration, perform the following steps:

> **Note:**
>
> These steps are applicable only to AD. No separate process is required to improve Reset Password Performance operation for OUD/OID.

1. Create the `SSO.RESETPASSWORDONTARGETBYPASSINGCONNECTOR` system property and set it to `true`.
2. Import the AD certificate into Oracle Identity Governance (OIG):
   - If Demo identity and trust store is used then import the AD certificate into Demo trust keystore:

     ```
     $JAVA_HOME/jre/bin/keytool -import -alias ad_trusted_cert -
     file $CERT_FILE
     -keystore $MW_HOME/wlserver/server/lib/DemoTrust.jks -storepass
     DemoTrustKeyStorePassPhrase
     ```

   - If custom identity and trust store is used then import the AD certificate into custom trust keystore:

     ```
     $JAVA_HOME/jre/bin/keytool -import -alias ad_trusted_cert -
     file $CERT_FILE
     -keystore $DOMAIN_HOME/config/fmwconfig/<CUSTOM_TRUST_STORE>.jks -
     storepass
     <CustomTrustKeyStorePassPhrase>
     ```

     > **Note:**
     >
     > You must place the custom trust keystore under `$DOMAIN_HOME/config/fmwconfig` and it must be file-based.

3.5 Scheduled Jobs for OIG-OAM Integration

OIG offers two sets of scheduled jobs for synchronizing with LDAP: Reconciliation Jobs and SSO Post Enable Jobs.

Reconciliation Jobs

The following reconciliation jobs are provided:

- SSO User Full Reconciliation
- SSO User Incremental Reconciliation
- SSO User Delete Reconciliation

> **Note:**
>
> The SSO User Delete Reconciliation scheduled job is available only after you apply OIM BUNDLE PATCH 12.2.1.4.200505.

- SSO Group Create and Update Full Reconciliation
- SSO Group Create and Update Incremental Reconciliation
- SSO Group Delete Full Reconciliation
- SSO Group Delete Incremental Reconciliation
- SSO Group Membership Full Reconciliation
- SSO Group Membership Incremental Reconciliation
- SSO Group Hierarchy Sync Full Reconciliation
- SSO Group Hierarchy Sync Incremental Reconciliation

> **Note:**
>
> SSO Group Hierarchy Sync Incremental Reconciliation is supported *only* for Oracle Internet Directory and Oracle Unified Directory.

Parameter Values for Reconciliation Jobs

Table 3-9 Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO User Full Reconciliation	Resource Object Name	SSOTarget	Name of the target resource object against which reconciliation runs must be performed. This corresponds to the target account which has to be reconciled for the user. This value is equal to the target application instance name**.**
SSO User Full Reconciliation	IT Resource Name	SSOTarget	Name of the target IT resource instance that the connector must use to reconcile data. This corresponds to the target account which has to be reconciled for the user. This value is equal to the target application instance name**.**
SSO User Full Reconciliation	Object Type	User	This attribute holds the type of object you want to reconcile. This value is fixed.
SSO User Full Reconciliation	Trusted Resource Object Name	SSOTrusted-for-SSOTarget	Name of the trusted resource object against which reconciliation runs must be performed. This corresponds to the target account which has to be reconciled for the user. This value is equal to the trusted application instance name (auto-generated by OIGOAMIntegrationScript.sh)**.**

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO User Full Reconciliation	Trusted IT Resource Name	SSOTrusted-for-SSOTarget	Name of the trusted IT resource instance that the connector must use to reconcile data. This corresponds to the target account which has to be reconciled for the user. This value is equal to the trusted application instance name (auto-generated by OIGOAMIntegrationScript.sh)**.**
SSO User Full Reconciliation	Scheduled Task Name	SSO User Full Reconciliation	This attribute holds the name of the scheduled ***job.*** This value is **fixed**.
SSO User Full Reconciliation	Incremental Recon Attribute	NA	This attribute should be left empty for SSO User Full Reconciliation job
SSO User Full Reconciliation	Latest Token	NA	This attribute should be left empty for SSO User Full Reconciliation job
SSO User Full Reconciliation	Sync Token	NA	This attribute should be left empty for SSO User Full Reconciliation job
SSO User Full Reconciliation	Filter	NA	Expression for filtering records that must be reconciled by the scheduled job. Sample value: startsWith('cn','Samrole1') Default value: None See Section 7.8 ICF Filter Syntax in Integrating ICF with Oracle Identity Governance documentation for the syntax of this expression.
SSO User Incremental Reconciliation	Resource Object Name	SSOTarget	Name of the target resource object against which reconciliation runs must be performed. This corresponds to the target account which has to be reconciled for the user. This value is equal to the target application instance name**.**
SSO User Incremental Reconciliation	IT Resource Name	SSOTarget	Name of the target IT resource instance that the connector must use to reconcile data. This corresponds to the target account which has to be reconciled for the user. This value is equal to the target application instance name**.**
SSO User Incremental Reconciliation	Object Type	User	This attribute holds the type of object you want to reconcile. This value is fixed.

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO User Incremental Reconciliation	Trusted Resource Object Name	SSOTrusted-for-SSOTarget	Name of the trusted resource object against which reconciliation runs must be performed. This corresponds to the target account which has to be reconciled for the user. This value is equal to the trusted application instance name (auto-generated by OIGOAMIntegrationScript.sh)**.**
SSO User Incremental Reconciliation	Trusted IT Resource Name	SSOTrusted-for-SSOTarget	Name of the trusted IT resource instance that the connector must use to reconcile data. This corresponds to the target account which has to be reconciled for the user. This value is equal to the trusted application instance name (auto-generated by OIGOAMIntegrationScript.sh)**.**
SSO User Incremental Reconciliation	Scheduled Task Name	SSO User Full Reconciliation	This attribute holds the name of the scheduled ***job.*** This value is **fixed**.
SSO User Incremental Reconciliation	Incremental Recon Attribute		Name of the target system attribute that holds the change number at which the last reconciliation run started. The value in this attribute is used during incremental reconciliation to determine the newest or latest record reconciled from the target system. This value is fixed.
SSO User Incremental Reconciliation	Latest Token		This attribute holds the value of the uSNChanged attribute of a domain controller that is used for reconciliation. Note: The reconciliation engine automatically enters a value for this attribute. It is recommended that you do not change the value of this attribute. If you manually specify a value for this attribute, then only group whose uSNChanged value is greater than the Latest Token attribute value are reconciled. Default value: None

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO User Incremental Reconciliation	Sync Token		This job parameter is only present if the target directory is Oracle Internet Directory or Oracle Unified Directory. You can manually enter the first Sync Token. To retrieve this token, query cn=changelog on rootDSE on the target system. Then, every time sync reconciliation is run, Sync Token is updated. Browse the changelog attribute of the target system to determine a value from the changelog that must be used to resume a reconciliation run. From the next reconciliation run onward, only data about records that are created or modified since the last reconciliation run ended are fetched into Oracle Identity Governance. Or, you can also leave this field blank, which causes the entire changelog to be read. This attribute stores values in one of the following formats: If you are using a target system for which the value of the standardChangelog entry in the Configuration lookup definition is set to true, then this attribute stores values in the following format: <Integer>VALUE</Integer> Sample value: <Integer>476</Integer> If you are using a target system (for example, OUD) for which the value of the standardChangelog entry in the Configuration lookup definition is set to false, then this attribute stores values in the following format: <String>VALUE</String> Sample value: <String>dc=example,dc=com:0000013633e514427b6600000013;</String> Default value: None
SSO User Incremental Reconciliation	Filter		Default value: None Expression for filtering records that must be reconciled by the scheduled job. Sample value: startsWith('cn','Samrole1') Default value: None See Section 7.8 ICF Filter Syntax in Integrating ICF with Oracle Identity Governance documentation for the syntax of this expression.

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO User Delete Reconciliation	Resource Object Name	SSOTarget	Name of the target resource object against which reconciliation runs must be performed. This corresponds to the target account, which is to be reconciled for the user. This value is equal to the target application instance name.
SSO User Delete Reconciliation	IT Resource Name	SSOTarget	Name of the target IT resource instance that the connector must use to reconcile data. This corresponds to the target account, which is to be reconciled for the user. This value is equal to the target application instance name.
SSO User Delete Reconciliation	Object Type	User	This attribute holds the type of object you want to reconcile. This value is fixed.
SSO User Delete Reconciliation	Trusted Resource Object Name	SSOTrusted-for-SSOTarget	Name of the trusted resource object against which reconciliation runs must be performed. This corresponds to the target account, which is to be reconciled for the user. This value is equal to the trusted application instance name (auto-generated by OIGOAMIntegrationScript.sh).
SSO User Delete Reconciliation	Trusted IT Resource Name	SSOTrusted-for-SSOTarget	Name of the trusted IT resource instance that the connector must use to reconcile data. This corresponds to the target account, which is to be reconciled for the user. This value is equal to the trusted application instance name (auto-generated by OIGOAMIntegrationScript.sh).
SSO User Delete Reconciliation	Scheduled Task Name	SSO Connector Integration User Delete Reconciliation	This attribute holds the name of the scheduled job. This value is fixed.
SSO Group Create and Update Full Reconciliation	Resource Object Name	SSO Group	Name of the resource object against which reconciliation runs must be performed This value is **fixed.**
SSO Group Create and Update Full Reconciliation	Object Type	Group	This attribute holds the type of object you want to reconcile. This value is fixed.
SSO Group Create and Update Full Reconciliation	IT Resource Name	SSO Server	Name of the IT resource instance that the connector must use to reconcile data. This value is fixed.

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO Group Create and Update Full Reconciliation	Scheduled Task Name	SSO Group Create And Update Full Reconciliation	This attribute holds the name of the scheduled ***job.*** This value is **fixed**.
SSO Group Create and Update Full Reconciliation	Filter		Expression for filtering records that must be reconciled by the scheduled job. Sample value: startsWith('cn','Samrole1') Default value: None See Section 7.8 ICF Filter Syntax in Integrating ICF with Oracle Identity Governance documentation for the syntax of this expression.
SSO Group Create and Update Full Reconciliation	Organization Name	Top	This job parameter is only present if the target directory is Active Directory. OIG Organization to which the reconciled role should be provisioned. This value is **fixed.**
SSO Group Create and Update Full Reconciliation	Organization Type	Company	This job parameter is only present if the target directory is Active Directory. Type of the organization to which the reconciled role is being provisioned. This attribute is used only with in connector reconciliation scope and does not have significance in OIG. This value is **fixed.**
SSO Group Create and Update Incremental Reconciliation	Resource Object Name	SSO Group	Name of the resource object against which reconciliation runs must be performed This value is **fixed.**
SSO Group Create and Update Incremental Reconciliation	Object Type	Group	This attribute holds the type of object you want to reconcile. This value is fixed.
SSO Group Create and Update Incremental Reconciliation	IT Resource Name	SSO Server	Name of the IT resource instance that the connector must use to reconcile data. This value is fixed.
SSO Group Create and Update Incremental Reconciliation	Scheduled Task Name	SSO Group Create And Update Incremental Reconciliation	This attribute holds the name of the scheduled ***job*****.** This value is **fixed**.

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO Group Create and Update Incremental Reconciliation	Filter		Expression for filtering records that must be reconciled by the scheduled job. Sample value: startsWith('cn','Samrole1') Default value: None See Section 7.8 ICF Filter Syntax in Integrating ICF with Oracle Identity Governance documentation for the syntax of this expression.
SSO Group Create and Update Incremental Reconciliation	Sync Token		This job parameter is only present if the target directory is Oracle Internet Directory or Oracle Unified Directory. You can manually enter the first Sync Token. To retrieve this token, query cn=changelog on rootDSE on the target system. Then, every time sync reconciliation is run, Sync Token is updated. Browse the changelog attribute of the target system to determine a value from the changelog that must be used to resume a reconciliation run. From the next reconciliation run onward, only data about records that are created or modified since the last reconciliation run ended are fetched into Oracle Identity Governance. Or, you can also leave this field blank, which causes the entire changelog to be read. This attribute stores values in one of the following formats: If you are using a target system for which the value of the standardChangelog entry in the Configuration lookup definition is set to true, then this attribute stores values in the following format: <Integer>VALUE</Integer> Sample value: <Integer>476</Integer> If you are using a target system (for example, OUD) for which the value of the standardChangelog entry in the Configuration lookup definition is set to false, then this attribute stores values in the following format: <String>VALUE</String> Sample value: <String>dc=example,dc=com:0000013633e514427b6600000013;</String> Default value: None

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO Group Create and Update Incremental Reconciliation	Incremental Recon Attribute	uSNChanged	This job parameter is only present if the target directory is Active Directory. Name of the target system attribute that holds the change number at which the last reconciliation run started. The value in this attribute is used during incremental reconciliation to determine the newest or latest record reconciled from the target system. This value is fixed.
SSO Group Create and Update Incremental Reconciliation	Latest Token		This attribute holds the value of the uSNChanged attribute of a domain controller that is used for reconciliation. Note: The reconciliation engine automatically enters a value for this attribute. It is recommended that you do not change the value of this attribute. If you manually specify a value for this attribute, then only group whose uSNChanged value is greater than the Latest Token attribute value are reconciled. Default value: None
SSO Group Create and Update Incremental Reconciliation	Organization Name	Top	This job parameter is only present if the target directory is Active Directory. OIG Organization to which the reconciled role should be provisioned. This value is **fixed.**
SSO Group Create and Update Incremental Reconciliation	Organization Type	Company	This job parameter is only present if the target directory is Active Directory. Type of the organization to which the reconciled role is being provisioned. This attribute is used only with in connector reconciliation scope and does not have significance in OIG. This value is **fixed.**
SSO Group Delete Full Reconciliation	IT Resource Name	SSO Server	Name of the IT resource instance that the connector must use to reconcile data. This value is fixed.
SSO Group Delete Full Reconciliation	Object Type	Group	This parameter holds the type of object you want to reconcile. This value is fixed.
SSO Group Delete Full Reconciliation	Resource Object Name	SSO Group	Name of the group resource object against which reconciliation runs must be performed This value is **fixed.**

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO Group Delete Full Reconciliation	Scheduled Task Name	SSO Group Delete Full Reconciliation	This attribute holds the name of the scheduled ***job.*** This value is **fixed**.
SSO Group Delete Full Reconciliation	Delete Recon	yes	This parameter is present only in SSO Group Delete Reconciliation for Active Directory. This value is **fixed.**
SSO Group Delete Full Reconciliation	Organization Name		This parameter is present only in SSO Group Delete Reconciliation for Active Directory. This value can be left empty.
SSO Group Delete Incremental Reconciliation	IT Resource Name	SSO Server	Name of the IT resource instance that the connector must use to reconcile data. This value is fixed.
SSO Group Delete Incremental Reconciliation	Object Type	Group	This attribute holds the type of object you want to reconcile. This value is fixed.
SSO Group Delete Incremental Reconciliation	Resource Object Name	SSO Group	Name of the group resource object against which reconciliation runs must be performed This value is **fixed.**
SSO Group Delete Incremental Reconciliation	Scheduled Task Name	SSO Group Delete Full Reconciliation	This attribute holds the name of the scheduled ***job.*** This value is **fixed**.

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO Group Delete Incremental Reconciliation	Sync Token		This job parameter is only present if the target directory is Oracle Internet Directory or Oracle Unified Directory. You can manually enter the first Sync Token. To retrieve this token, query cn=changelog on rootDSE on the target system. Then, every time sync reconciliation is run, Sync Token is updated. Browse the changelog attribute of the target system to determine a value from the changelog that must be used to resume a reconciliation run. From the next reconciliation run onward, only data about records that are created or modified since the last reconciliation run ended are fetched into Oracle Identity Governance. Or, you can also leave this field blank, which causes the entire changelog to be read. This attribute stores values in one of the following formats: If you are using a target system for which the value of the standardChangelog entry in the Configuration lookup definition is set to true, then this attribute stores values in the following format: <Integer>VALUE</Integer> Sample value: <Integer>476</Integer> If you are using a target system (for example, OUD) for which the value of the standardChangelog entry in the Configuration lookup definition is set to false, then this attribute stores values in the following format: <String>VALUE</String> Sample value: <String>dc=example,dc=com:0000013633e514427b6600000013;</String> Default value: None
SSO Group Delete Incremental Reconciliation	Delete Recon	yes	This parameter is present only in SSO Group Delete Reconciliation for Active Directory. This value is **fixed**.
SSO Group Delete Incremental Reconciliation	Organization Name		This parameter is present only in SSO Group Delete Reconciliation for Active Directory. This value can be empty.

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO Group Membership Full Reconciliation	Application Name	SSOTarget	Name of the target application name from which you reconcile records
SSO Group Membership Full Reconciliation	Object Type	User	This attribute holds the type of object you want to reconcile. This value is fixed.
SSO Group Membership Full Reconciliation	IT Resource Name	SSOTarget	Name of the IT resource user by target application instance from which you reconcile records.
SSO Group Membership Full Reconciliation	Scheduled Task Name	SSO Group Membership Full Reconciliation	This attribute holds the name of the scheduled ***job.*** This value is **fixed**.
SSO Group Membership Full Reconciliation	Filter	<Empty>	Expression for filtering records that must be reconciled by the scheduled job. Sample value: startsWith('cn','Samrole1') Default value: None See Section 7.8 ICF Filter Syntax in Integrating ICF with Oracle Identity Governance documentation for the syntax of this expression.
SSO Group Membership Incremental Reconciliation	Application Name	SSOTarget	Name of the target application name from which you reconcile records
SSO Group Membership Incremental Reconciliation	Resource Object Name	SSO Group	Name of the group resource object against which reconciliation runs must be performed This value is **fixed.**
SSO Group Membership Incremental Reconciliation	IT Resource Name	SSO Server	Name of the IT resource instance that the connector must use to reconcile data. This value is fixed.
SSO Group Membership Incremental Reconciliation	User IT Resource Name	SSOTarget	Name of the IT resource used by target application instance installation from which you reconcile records. This would be same as target application instance

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO Group Membership Incremental Reconciliation	User Resource Object Name	SSOTarget	Resource Object name corresponding to target application instance. This would be same as target application instance
SSO Group Membership Incremental Reconciliation	Scheduled Task Name	SSO Group Membership Incremental Reconciliation	Fixed for this job. Not changeable
SSO Group Membership Incremental Reconciliation	Object Type	Group	This attribute holds the type of object you want to reconcile. This value is fixed.

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO Group Membership Incremental Reconciliation	Sync Token		This job parameter is only present if the target directory is Oracle Internet Directory or Oracle Unified Directory. You can manually enter the first Sync Token. To retrieve this token, query cn=changelog on rootDSE on the target system. Then, every time sync reconciliation is run, Sync Token is updated. Browse the changelog attribute of the target system to determine a value from the changelog that must be used to resume a reconciliation run. From the next reconciliation run onward, only data about records that are created or modified since the last reconciliation run ended are fetched into Oracle Identity Governance. Or, you can also leave this field blank, which causes the entire changelog to be read. This attribute stores values in one of the following formats: If you are using a target system for which the value of the standardChangelog entry in the Configuration lookup definition is set to true, then this attribute stores values in the following format: <Integer>VALUE</Integer> Sample value: <Integer>476</Integer> If you are using a target system (for example, OUD) for which the value of the standardChangelog entry in the Configuration lookup definition is set to false, then this attribute stores values in the following format: <String>VALUE</String> Sample value: <String>dc=example,dc=com:0000013633e514427b6600000013;</String> Default value: None
SSO Group Membership Incremental Reconciliation	Incremental Recon Attribute	uSNChanged	This job parameter is only present if the target directory is Active Directory. Name of the target system attribute that holds the change number at which the last reconciliation run started. The value in this attribute is used during incremental reconciliation to determine the newest or latest record reconciled from the target system. This value is fixed.

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO Group Membership Incremental Reconciliation	Latest Token		This attribute holds the value of the uSNChanged attribute of a domain controller that is used for reconciliation. Note: The reconciliation engine automatically enters a value for this attribute. It is recommended that you do not change the value of this attribute. If you manually specify a value for this attribute, then only group whose uSNChanged value is greater than the Latest Token attribute value are reconciled. Default value: None
SSO Group Membership Incremental Reconciliation	Filter		Expression for filtering records that must be reconciled by the scheduled job. Sample value: startsWith('cn','Samrole1') Default value: None See Section 7.8 ICF Filter Syntax in Integrating ICF with Oracle Identity Governance documentation for the syntax of this expression.
SSO Group Hierarchy Full Reconciliation	Resource Object Name	SSO Group	Name of the resource object against which reconciliation runs must be performed This value is **fixed.**
SSO Group Hierarchy Full Reconciliation	Object Type	Group	This attribute holds the type of object you want to reconcile. This value is fixed.
SSO Group Hierarchy Full Reconciliation	IT Resource Name	SSO Server	Name of the IT resource instance that the connector must use to reconcile data. This attribute holds the type of object you want to reconcile. This value is fixed.
SSO Group Hierarchy Full Reconciliation	Scheduled Task Name	SSO Group Hierarchy Full Reconciliation	This attribute holds the name of the scheduled ***job.*** This value is **fixed**.
SSO Group Hierarchy Full Reconciliation	Sync Token		This value should always be empty for SSO Group Hierarchy Full Reconciliation
SSO Group Hierarchy Incremental Reconciliation	Resource Object Name	SSO Group	Name of the resource object against which reconciliation runs must be performed This value is **fixed.**

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO Group Hierarchy Incremental Reconciliation	Object Type	Group	This attribute holds the type of object you want to reconcile. This value is **fixed.**
SSO Group Hierarchy Incremental Reconciliation	IT Resource Name	SSO Server	Name of the IT resource instance that the connector must use to reconcile data. This value is fixed.
SSO Group Hierarchy Incremental Reconciliation	Scheduled Task Name	SSO Group Hierarchy Full Reconciliation	This attribute holds the name of the scheduled ***job.*** This value is **fixed**.

Table 3-9 (Cont.) Parameter values for reconciliation jobs

Reconciliation job	Parameter Name	Parameter Value	Description
SSO Group Hierarchy Incremental Reconciliation	Sync Token		This job parameter is only present if the target directory is Oracle Internet Directory or Oracle Unified Directory. You can manually enter the first Sync Token. To retrieve this token, query cn=changelog on rootDSE on the target system. Then, every time sync reconciliation is run, Sync Token is updated. Browse the changelog attribute of the target system to determine a value from the changelog that must be used to resume a reconciliation run. From the next reconciliation run onward, only data about records that are created or modified since the last reconciliation run ended are fetched into Oracle Identity Governance. Or, you can also leave this field blank, which causes the entire changelog to be read. This attribute stores values in one of the following formats: If you are using a target system for which the value of the standardChangelog entry in the Configuration lookup definition is set to true, then this attribute stores values in the following format: <Integer>VALUE</Integer> Sample value: <Integer>476</Integer> If you are using a target system (for example, OUD) for which the value of the standardChangelog entry in the Configuration lookup definition is set to false, then this attribute stores values in the following format: <String>VALUE</String> Sample value: <String>dc=example,dc=com:0000013633e514427b6600000013;</String> Default value: None

SSO Post Enable Jobs

OIG offers post enable jobs to seed identities and their relation from OIG to LDAP.

The post enable jobs are to be used in case of following deployment scenario: OIG is already been in deployment for certain period of time and OIG is now being integrated with OAM and LDAP. During such scenarios, the existing users and roles and their relations in OIG needs to seeded to synchronize LDAP with data in OIG. After OIG-OAM integration configuration has been performed, these jobs should be run once to seed the users, roles and their relationships to LDAP.

The following post enable jobs are offered:

- SSO Post Enable Provision Users to LDAP:

  For each user in OIG, this job creates an user in LDAP and provisions SSO target application instance to the user.

- SSO Post Enable Provision Roles to LDAP:

  For each role in OIG, this job creates a role in LDAP and subsequently creates a lookup, entitlement and catalog entry for the entitlement.

- SSO Post Enable Provision Role Membership to LDAP:

  For each role granted to the user, this job grants entitlement (corresponding to the role) and in-turn grants the membership for the user in LDAP.

- SSO Post Enable Provision Role Hierarchy to LDAP:

  For each role-role relation in OIG, this job adds relationship for the groups in LDAP.

Reconciliation Behavior

User Reconciliation

User reconciliation reconciles user (and account) from the LDAP. For each user reconciled, it provisions SSO target application instance to the reconciled user. User reconciliation job reconciles users that have following objectclasses:

- InetOrgPerson
- orclIDXPerson
- OblixOrgPerson
- OblixPersonPwdPolicy
- OIMPersonPwdPolicy

For user reconciliation, set the value for the two mandatory attributes: `sn` and `uid`.

User Matching rule:

User reconciliation job uses following reconciliation matching rule for creating or updating users in OIG:

```
<matchingRule>((UPPER(USR.usr_ldap_guid)=UPPER(RA_SSOTRUSTEDFORSSAEC4C34A.RA_LDAP
GUID94FE1B62)) OR
(UPPER(USR.usr_login)=UPPER(RA_SSOTRUSTEDFORSSAEC4C34A.RA_USERLOGIN7C7B96D4)))</
matchingRule>
```

Account Matching rule:

User reconciliation job uses following reconciliation matching rule for provisioning SSO target application instance account to a user in OIG:

```
<matchingRule>((UPPER(USR.usr_login)=UPPER(RA_SSOTARGE.RA_USERLOGIN7C7B96D4)) OR
(UPPER(USR.usr_ldap_guid)=UPPER(RA_SSOTARGE.RA_ORCLGUID)))</matchingRule>
```

Group Reconciliation

Group reconciliation job reconciles groups that have following two objectclass:

- groupOfUniqueNames - in case of OID and OUD
- group - in case of AD

Group reconciliation job requires that group names are unique in OIG. That is, when the job reconciles a create changelog for a group with name 'Business Administrator' and if OIG already has a role with name 'Business Administrator', then Business Administrator group would not be created again in OIG and the reconciled role will be skipped from further processing.

Alternatively, if a group exists in OIG that has a matching GUID with the group being reconciled from LDAP, then reconciliation engine would perform an update for the existing group in OIG.

Group Matching Rule:

```
<matchingRule>(UD_SSO_GR.UD_SSO_GR_SERVER=RA_SSOGROUP4DF6ECEE.RA_ITRESOURCENAME70C9F928
 and UD_SSO_GR.UD_SSO_GR_ORCLGUID=RA_SSOGROUP4DF6ECEE.RA_ORCLGUID)</matchingRule>
```

Group Membership Reconciliation

Group membership reconciliation reconciles the current role grants for user in LDAP. On successful reconciliation, for each role granted to the user, an entitlement corresponding to the role is assigned to the user's SSO account.

Entitlement assignment to the user during reconciliation is executed by database trigger for child form table. This child form table stores the membership grants for the user (i.e. account). In some circumstances, the entitlement assignment trigger may not have executed and hence, the user may not have the entitlement assignment yet corresponding to the role grant reconciliation. In such scenarios, execute 'Entitlement Assignment' job to assign entitlements.

Group Hierarchy Reconciliation

Group hierarchy reconciliation job reconcilies current role relations from LDAP.

Reconciliation Job Errors and Remedial Actions

- Group membership reconciliation
- Group hierarchy reconciliation

Group membership reconciliation

Group membership Full reconciliation

- The user entry which is reconciled is looked up in OIG corresponding to its GUID. If no matching user is found, recon event creation for that user entry is skipped and an error message corresponding to the skipped user entry is added to job error messages.
- If the user entry is present but one of the parent roles, with matching role DN, is not existing in OIG, then recon event creation for that user entry is skipped and an error message corresponding to the skipped user entry is added to job error messages.

If there are no missing parent roles for a user entry, then recon event is created for the user entry and added to batch recon service. Once reconciliation job, error message is set for the Job ID.

Group membership Incremental reconciliation

Group membership incremental reconciliation has same behavior as group membership full reconciliation. In addition to reporting the error message, incremental reconciliation also doesn't update the latest incremental token. This is to ensure that when the job is re-run (after performing remedy actions such as running user or group reconciliation jobs), then the user

entry(s) which were skipped earlier are assigned a recon event during their next error-free execution.

In situations where customer decide to bypass the error-encountered user entry and want to run incremental reconciliation with latest incremental token, they can do so by checking the schedule job error message from the job UI and the latest token will be printed at the end of the error message. Refer 'Example for reconciliation error due to missing user or role'

Group hierarchy reconciliation

Group Hierarchy Full reconciliation

- The role entry which is reconciled is looked up in OIG corresponding to its GUID. If no matching role is found, recon event creation for that role entry is skipped and an error message corresponding to the skipped user entry is added to job error messages
- If the role entry is present but one of the child roles, with matching role DN, is not existing in OIG, then recon event creation for the parent role entry is skipped and an error message corresponding to the skipped user entry is added to job error messages.

If there are no missing parent or child roles, then recon event is created for the parent role entry and added to batch recon service.

Once reconciliation job completes, error message is set for the Job ID.

Group Hierarchy Incremental reconciliation

Group hierarchy incremental reconciliation has same behavior as group hierarchy full reconciliation. In addition to reporting the error message if dataErrorDetected is true, incremental reconciliation also doesn't update the latest incremental token. This is to ensure that when the job is re-run (after performing remedy actions), then the role entry(s) which were skipped earlier are assigned a recon event during their next error-free execution.

In situations where customer decide to bypass the error-encountered role entry and want to run hierarchy incremental reconciliation with latest incremental token, they can do so by checking the schedule job error message from the job UI and the latest token will be printed at the end of the error message.

Example for Reconciliation Error due to Missing User or Role

Let's assume Group Membership Incremental Reconciliation is executed and the scheduled task identifies that some of the groups, whose membership is to be reconciled, doesn't exists in OIG yet. In such scenario, the scheduled task skips the creation of recon event for the role and adds the GUID of the role to the list of data error messages. Once all the group changelog has been processed, the scheduled task proceeds to submit batch reconciliation for the roles that did not encounter such error (i.e. did not encounter role or user not existing in OIG). For the roles that encountered error, the scheduled task compiles the error message and throws an exception. The outcome is:

```
The scheduled job status would be failed.
```

For the job that failed, the 'View error details' would have the list of the roles that were skipped. The last line of the message will have the latest incremental token that was processed by the scheduled task. Sample error message:

```
oracle.iam.connectors.icfcommon.exceptions.OIMException:
Role with GUID 54A78A7F44E41C39E053211CF50A7639 does not exist in OIM. Skipping group
membership incremental reconciliation for the role
Role with GUID 5E750AB0341F16D3E053211CF50A866D does not exist in OIM. Skipping group
membership incremental reconciliation for the role
Role with GUID 5E750AB0342016D3E053211CF50A866D does not exist in OIM. Skipping group
membership incremental reconciliation for the role
Role with GUID 5E750AB0346116D3E053211CF50A866D does not exist in OIM. Skipping group
membership incremental reconciliation for the role
Role with GUID 5E750AB0346216D3E053211CF50A866D does not exist in OIM. Skipping group
membership incremental reconciliation for the role
Role with DN cn=SYSTEM ADMINISTRATORS,cn=Groups,dc=us,dc=oracle,dc=com is not found in
OIM - Skipping group membership reconciliation for the user with GUID:
5376289A3A766EE7E053211CF50A8B24.
Latest Token value: <Integer>4204</Integer>
```

Corrective Actions for Reconciliation Error

- Customer can execute 'SSO Group Create or Update Reconciliation' job to fix the above errors and re-run group membership incremental reconciliation job. Similarly, execute 'SSO User Reconciliation' job if the error message relates to 'user not existing in OIG'.
- Alternatively, if customer prefer to ignore the error for these roles and would like to proceed beyond with **incremental reconciliation** in future, then customer can set the Sync Token job parameter value to the latest token value listed in the error message. For example, for the above sample message, the Sync Token job parameter value would be: <Integer>4204</Integer>
- In case of group membership full reconciliation or group hierarchy full reconciliation, if any of the user(s) and/or group(s) reconciled does not exist in OIG, then the job would report failed status for the missing user and/or group in all subsequent runs.

Ensuring identity Tables Data Synchronization With Child Form Tables

During group membership reconciliation and group hierarchy reconciliation, the reconciliation engine updates the child form table corresponding to each recon event data in reconciliation batch. When reconciliation engine triggers post process orchestration for each reconciliation batch, the post process handlers fetches the child form entry corresponding to each recon event in batch and updates OIG's identity relation tables.

Under situations where reconciliation post process handler fails to synchronize the child form data with identity table, it is possible to remediate the data inconsistence between the tables by executing following jobs:

- Sync Group Membership with SSO Form Table:

  For each user in parent form, this job synchronizes membership child form data with USG table. This job accepts an 'Group Membership Child Form Table' name as input parameter and it is assigned a default value. If membership child form table name is different in customer's deployment, then this parameter has to be assigned with appropriate value.
- Sync Group Hierarchy with SSO Form Table:

  For each role in parent form, this job synchronizes role relationship data with GPG table. Child form table name for role relationship is fixed for a deployment and hence, this job does not accept child form table name as input.

3.6 Configuring User Defined Fields

This section contains the following topics:

- Configuring User Defined Fields with SSO
- Configuring Role UDFs

3.6.1 Configuring User Defined Fields with SSO

You can configure custom attributes or user-defined fields (UDFs) with SSO.

To do so, complete the following steps:

1. Create the UDFs for OIG. For more information, see Creating a Custom Attribute.

> **Note:**
>
> Do not specify any value for the LDAP Attribute in the Create Text Field page.

2. Add the UDF into the Create User Form. For more information, see Adding a Custom Attribute Category into Create User Form in *Administering Oracle Identity Governance*.
3. Add UDF to the SSO target application instance. For more information, see Adding Attribute in *Performing Self Service Tasks with Oracle Identity Governance*.
4. Add UDF to the SSO trusted application instance. For more information, see Providing Schema Information for Authoritative Application in *Performing Self Service Tasks with Oracle Identity Governance*.

3.6.2 Configuring Role UDFs

The configuring Role UDF enhancement is supported for the following integrations:

- OIM-OAM integration setup created using Integrating OIG with OAM and LDAP Connectors.
- LDAP Connector Sync support for non OAM installations using `Doc ID 2833544.1` at https://support.oracle.com.

> **Note:**
>
> Before configuring role UDFs, apply the latest bundle patch available for your release.

To configure role UDFs, complete the following steps:

1. Create UDFs for OIG Role entity. For more information, see Configuring Custom Attributes .
2. Define the Reconciliation mapping for the created role UDFs. Table 3-10 lists the exact entity names to be used while defining the reconciliation mapping.

> **Note:**
>
> - For more information on defining reconciliation mapping for AD, see Adding Custom Fields for Target Resource Reconciliation of Groups and Organizational Units.
> - For more information on defining reconciliation mapping for OUD/OID, see Adding the Custom Field to Resource Object Reconciliation Fields.

3. Define the Provisioning mapping for this role UDF. Table 3-10 lists the exact entity names to be used while defining the provisioning mapping.

> **Note:**
>
> - For more information on defining provisioning mapping for AD, see Adding Custom Fields for Provisioning Groups and Organizational Units.
> - For more information on defining provisioning mapping for OUD/OID, see Adding the new Field to the Process Form.

4. Log in to Oracle Identity System Administrator.
5. Open the **Lookup.RoleAttrFormField.Map** file and set the Code and Meaning field values, where:
   - **Code** – Refers to the OIM Role Entity's attribute that is, UDF.
   - **Meaning** – Refers to Process Form field name defined in design console.

> **Note:**
>
> - The **Code** and **Meaning** in the **Lookup.RoleAttrFormField.Map** must be the same as that is created in Form and Role UDF.
> - If the lookup file does not exist, then create a new lookup file and then update the values. For more information on creating and updating the lookup, see Managing Lookups.

All the required mappings are done now to map the Role UDF to the target field.

Table 3-10 Reconciliation and Provisioning Mapping

LDAP Directory	Resource Object Name	UAD Table Name	Provisioning Lookup	Reconciliation Lookup	Adapter
AD	SSO Group	UD_SSOGRP	Lookup.SSO.GM.ProvAttrMap	Lookup.SSO.GM.ReconAttrMap	adpSSOADIDCUPDATEATTRIBUTEVALUE
OUD	SSO Group	UD_SSO_GR	Lookup.SSO.Group.ProvAttrMap	Lookup.SSO.Group.ReconAttrMap	adpSSOLDAPUPDATE

Table 3-10 (Cont.) Reconciliation and Provisioning Mapping

LDAP Directory	Resource Object Name	UAD Table Name	Provisioning Lookup	Reconciliation Lookup	Adapter
OID	SSO Group	UD_SSO_GR	Lookup.SSO.Group.ProvAttrMap	Lookup.SSO.Group.ReconAttrMap	adpSSOOIDUPDATE

The following points should be considered when configuring the Role UDFs with different data types:

- If you are creating role UDF mapping for the check box type UDF field and the mapped attribute on Target LDAP is storing values for a Boolean field as 'True' or 'False', then add a recon transformation script to convert the value 'True' to '1' and 'False' to '0' for successful Reconciliation. For more information on the steps to create a transformation script, see Transformation Script.
- To support the `Date` type of Role UDF which is mapped to the `Date` type of target field:
  - Add the field flag `[DATE]` to the Provisioning and Recon attribute Map. For example, `Joining Date[DATE]`.
  - For OID/OUD integration, update attribute `dateFormat` and `dateTypeAttrNames` in the lookup **Lookup.SSO.Configuration**.
  - For AD integration, update attribute `CustomDateAttributes` in the lookup **Lookup.Configuration.SSO**.

3.7 Known Limitations and Workarounds in OIG-OAM Integration

Learn more about the known issue and limitations in OIG-OAM Integration.

Some of the known limitation in OIG-OAM Integration:

- Do not request the SSO target application.
- Do not use SSO target application for access policy.
- Do not disable or manually remove the SSO target application.
- In an OIG-OAM integrated environment, do not add, modify, or remove entitlements that are associated with SSO target application from the Entitlements tab of a user details page or My Access page. Add, modify, or remove roles from the Role tab in the user detail page or My Access page.
- SSO target application UI forms are not available out-of-box. You can generate them from the Oracle Identity System Administration Console.
- When you clone a SSO target application, the new cloned application can be used for provisioning and reconciliation operations. Do not clone the SSO target application to support SSO integration.
- Role User-Defined Fields (UDFs) are not supported.
- When the integration environment is setup with AD, OUD, or OID as LDAP, the LDAP connector is configured with the application instance name `SSOTarget`. The

application instance name is configurable and is taken as your input in the `SSO_TARGET_APPINSTANCE_NAME` proprety value in the `configureLDAPConnector.config` file. Therefore, after OAM-OIG integration, open the SSO User Delete Reconciliation scheduled job in the Scheduler, and update the following parameter values with the application name as provided during integration:

- IT Resource Name
- Resource Object Name
- Trusted IT Resource Name
- Trusted Resource Object Name

For more Oracle Identity Governance Integration Issues and Workarounds, see Integration Issues and Workarounds in *Release Notes for Oracle Identity Management*.

4

Troubleshooting Common Problems in Access Manager and OIG Integration

These sections describe common problems you might encounter in an Oracle Identity Governance and Access Manager integrated environment and explain how to solve them.

- Troubleshooting Single Sign-On Issues in an Access Manager and OIG Integrated Environment
- Troubleshooting Auto-Login Issues in an Access Manager and OIG Integrated Environment
- Troubleshooting Session Termination Issues
- Troubleshooting Account Self-Locking Issues
- Troubleshooting Miscellaneous Issues in an Access Manager and OIG Integrated Environment
- Troubleshooting Target Account Creation
- Troubleshooting prepareIDStore for AD
- Troubleshooting the OIG-OAM Integrated Environment Upgrade

In addition to this section, review the *Error Messages* for information about the error messages you may encounter.

For information about additional troubleshooting resources, see Using My Oracle Support for Additional Troubleshooting Information.

4.1 Troubleshooting Single Sign-On Issues in an Access Manager and OIG Integrated Environment

This section describes common problems and solutions relating to single sign-on in the integrated environment. Using single sign-on, a user can access Oracle Identity Governance resources after being successfully authenticated by Access Manager. When accessing any Oracle Identity Governance resource protected by Access Manager, the user is challenged for their credentials by Access Manager using the Oracle Access Management Console login page.

This section discusses the following single sign-on issues:

- Diagnosing Single Sign-On Issues By Capturing HTTP Headers
- Access Manager Redirection to OIG Login Page
- Access Manager Failure to Authenticate User
- Troubleshooting Oracle Access Management Console Login Operation Errors
- Troubleshooting Authenticated User Redirection to OIG Login

- User Redirected to OIG During OIG Forgot Password, Register New Account, or Track User Registration Flows
- User Redirection in a Loop
- Troubleshooting SSO Integration Configuration

4.1.1 Diagnosing Single Sign-On Issues By Capturing HTTP Headers

Checking the HTTP headers may provide diagnostic information about login issues.You can collect information from the HTTP headers for troubleshooting issues. This can be done by enabling HTTP tracing in the web browser, logging into Access Manager as a new user, and examining the headers for useful information.

4.1.2 Access Manager Redirection to OIG Login Page

After accessing an Oracle Identity Governance resource using OHS (for example, `http://OHS_HOST:OHS_PORT/identity`), the user is redirected to the Oracle Identity Governance login page instead of the Oracle Access Management Console login page.

Cause

The Access Manager WebGate is not deployed or configured properly.

Solution

Confirm the `httpd.conf` file contains the following entry at the end:

```
"include "webgate.conf"
```

where `webgate.conf` contains the 12*c* WebGate configuration.

If this entry is not found, review the WebGate configuration steps to verify none were missed. For more information, see Configuring Oracle HTTP Server WebGate for Oracle Access Manager in *Installing WebGates for Oracle Access Manager* and Configuring Access Manager Settings in the *Administering Oracle Access Management*.

4.1.3 Access Manager Failure to Authenticate User

User login fails with the following error:

```
An incorrect Username or Password was specified.
```

Cause

Access Manager is responsible for user authentication but authentication has failed. The identity store configuration may be wrong.

Solution

Check that the identity store is configured correctly in the Oracle Access Management Console.

To resolve this problem:

1. Login to Oracle Access Management Console.

2. Navigate to **Configuration** >**User Identity Stores** > **OAMIDStore**.
3. Verify the Default Store and System Store configuration.
4. Click **Test Connection** to verify the connection.

4.1.4 Troubleshooting Oracle Access Management Console Login Operation Errors

User is not directed to the Oracle Access Management Console to login and the following error message appears:

```
Oracle Access Manager Operation Error.
```

Cause 1

The OAM Server is not running.

Solution 1

Start the OAM Server.

Cause 2

The WebGate is not correctly deployed on OHS and is not configured correctly for the 12*c* Agent located on the OAM Server.

An error message displays, for example: `The AccessGate is unable to contact any Access Servers.`

The issue may be with the SSO Agent.

See *Understanding Credential Collection and Login* in *Administering Oracle Access Management*.

Solution 2

To resolve this problem:

1. Run `oamtest.jar` (*`ORACLE_HOME`*`/idm/oam/server/tester`) and test the connection by specifying `AgentID`.

   The `AgentID` can be found in `ObAccessClient.xml`, located in the `webgate/config` directory in the *`WEBSERVER_HOME`*. For example:

   ```
   <SimpleList>

           <NameValPair

               ParamName="id"

               Value="IAMAG_11g"></NameValPair>

       </SimpleList>
   ```

   If the Tester fails to connect, this confirms a problem exists with the SSO Agent configuration (password/host/port) on the OAM Server.
2. Re-create the 12*c* SSO Agent and then reconfigure the WebGate to use this Agent.

4.1.5 Troubleshooting Authenticated User Redirection to OIG Login

User authenticated using the Oracle Access Management Console but is redirected to the Oracle Identity Governance login page to enter credentials.

Cause 1

The security providers for the OIG domain are not configured correctly in Oracle WebLogic Server.

Solution 1

Verify the WebLogic security providers are configured correctly for the OIG domain security realm. Check the LDAP Authenticator setting. For more information, see Validating the Oracle Identity Governance Security Provider Configuration.

Cause 2

`OAMIDAsserter` is not configured correctly in Oracle WebLogic Server.

Solution 2

To resolve this problem:

1. Log in to the WebLogic Server Administration Console for the OIG domain.
2. Navigate to **Security Realms**, **myrealm**, and then **Providers**.
3. Click **OAMIDAsserter**.
4. Navigate to **Common** tab and verify **Active Types** contains the correct header for the WebGate type:

   `OAM_REMOTE_USER` for WebGate 12*c*.

4.1.6 User Redirected to OIG During OIG Forgot Password, Register New Account, or Track User Registration Flows

Access Manager relies upon Oracle Identity Governance for password management. If the user logs in for the first time or if the user password is expired, Access Manager redirects the user to the Oracle Identity Governance First Login page.

From the Access Manager login screen, user should be able to navigate to the Oracle Identity Governance Forgot Password, the Self-Registration or Track Registration flows.

Cause

If there is any deviation or error thrown when performing these flows, the configuration in `oam-config.xml` (*`OAM_DOMAIN_HOME`*`/config/fmwconfig`) is incorrect. See Exporting and Importing the OAM Configuration File for the steps to export and import the `oam-config.xml` file.

Solution

Verify the contents of `oam-config.xml` resembles the following example. Specifically, that `HOST` and `PORT` corresponds to the OHS (or any supported web server) configured to front-end Oracle Identity Governance resources.

```
Setting Name="IdentityManagement" Type="htf:map">
<Setting Name="IdentityServiceConfiguration" Type="htf:map">
<Setting Name="IdentityServiceProvider"
Type="xsd:string">oracle.security.am.engines.idm.provider.OracleIdentityServiceProvider
</Setting>
<Setting Name="AnonymousAuthLevel" Type="xsd:integer">0</Setting>
<Setting Name="IdentityServiceEnabled" Type="xsd:boolean">true</Setting>
<Setting Name="IdentityServiceProviderConfiguration" Type="htf:map">
<Setting Name="AccountLockedURL" Type="xsd:string">/identity/faces/accountlocked</
Setting>
<Setting Name="ChallengeSetupNotDoneURL" Type="xsd:string">/identity/faces/firstlogin</
Setting>
<Setting Name="DateFormatPattern" Type="xsd:string">yyyy-MM-dd'T'HH:mm:ss'Z'</Setting>
<Setting Name="ForcedPasswordChangeURL" Type="xsd:string">/identity/faces/firstlogin</
Setting>
<Setting Name="IdentityManagementServer" Type="xsd:string">OIM-SERVER-1</Setting>
<Setting Name="PasswordExpiredURL" Type="xsd:string">/identity/faces/firstlogin</
Setting>
<Setting Name="LockoutAttempts" Type="xsd:integer">5</Setting>
<Setting Name="LockoutDurationSeconds" Type="xsd:long">31536000</Setting>
</Setting>
</Setting>
<Setting Name="RegistrationServiceConfiguration" Type="htf:map">
<Setting Name="RegistrationServiceProvider"
Type="xsd:string">oracle.security.am.engines.idm.provider.DefaultRegistrationServicePro
vider</Setting>
<Setting Name="RegistrationServiceEnabled" Type="xsd:boolean">true</Setting>
<Setting Name="RegistrationServiceProviderConfiguration" Type="htf:map">
<Setting Name="ForgotPasswordURL" Type="xsd:string">/identity/faces/forgotpassword</
Setting>
<Setting Name="NewUserRegistrationURL" Type="xsd:string">/identity/faces/register</
Setting>
<Setting Name="RegistrationManagementServer" Type="xsd:string">OIM-SERVER-1</Setting>
<Setting Name="TrackUserRegistrationURL" Type="xsd:string">/identity/faces/
trackregistration</Setting>
</Setting>
</Setting>
<Setting Name="ServerConfiguration" Type="htf:map">
<Setting Name="OIM-SERVER-1" Type="htf:map">
<Setting Name="Host" Type="xsd:string">myhost1.example.com</Setting>
<Setting Name="Port" Type="xsd:integer">7777</Setting>
<Setting Name="SecureMode" Type="xsd:boolean">false</Setting>
</Setting>
</Setting>
</Setting>
```

4.1.7 User Redirection in a Loop

A new user attempts to access Oracle Identity Management Self-Service and after successful authentication, the user is redirected in a loop. The service page does not load and the browser continues spinning or refreshing.

Cause

OHS configuration setting for `WLCookieName` for front-ending `identity` is incorrect.

Solution

Check the OHS configuration for front-ending `identity` and verify that `WLCookieName` directive is set to `oimjsessionid`. If not, set this directive as `oimjsessionid` for each Oracle Identity Management resource `Location` entry. For example:

```
<Location /identity>

  SetHandler weblogic-handler

  WLCookieName oimjsessionid

  WebLogicHost myhost1.example.com

  WebLogicPort 8003

  WLLogFile "$
Unknown macro: {ORACLE_INSTANCE}
/diagnostics/logs/mod_wl/oim_component.log"

  </Location>
```

4.1.8 Troubleshooting SSO Integration Configuration

Cause

During Configuring SSO Integration execution, the script could fail due to OAM-related issues:

Solution

1. Verify if OAM server is up.
2. Ensure that the credentials used for this step are correct.
3. Check from the console log if it is `Error 401--Unauthorized`.
4. Restart OAM admin and managed servers.
5. Ensure that the sso-config.properties file reflects the following:

```
generateIndividualConfigFiles=false
prepareIDStore=false
configOAM=false
addMissingObjectClasses=false
populateOHSRules=false
configureWLSAuthnProviders=false
configureLDAPConnector=false
configureSSOIntegration=true
enableOAMSessionDeletion=false
updateContainerRules=false
```

6. Run the following REST API and ensure it responds with the OAM policy application domains.

```
http(s)://<oam-admin-server-host>:<oam-admin-server-port>
/oam/services/rest/11.1.2.0.0/ssa/policyadmin/appdomain
```

> **Note:**
>
> The REST API must be run by the user having System Administrator privileges.

To assign system administrator role to a user, perform the following steps:

a. Log in to the OAM console.
b. Click **Configuration** > **Administration** > **Grant**.
c. Search for the user to whom you are required to provide system administrator privileges. For example, weblogic_idm
d. Ensure the **Role** is set to **System Administrator**.
e. Click **Add Selected**.
f. Go to the `configureSSOIntegration.config` file and specify the user with system administrator privileges against the `IDSTORE_OAMADMINUSER` property. For example, `IDSTORE_OAMADMINUSER =weblogic_idm`

If the REST endpoint does not respond, or returns `Request Failed` error, perform the following steps:

a. Login to the OAM AdminServer WLS Console.
b. Navigate to **Application Deployments**.
c. Select **oam-admin**, click **Update** and then click **Active**.
d. Stop all OAM domain servers.
e. Delete the `tmp` and cache directories under admin, oam and policy manager server.
f. Start all the oam domain servers and run the REST command again.

> **Note:**
>
> Do not progress to the next step unless the specified REST API responds with the OAM policy application domains. Otherwise, the following script may return `UnmarshalException`.

7. Run `OIGOAMIntegration.sh -configureSSOIntegration`.

4.1.9 WADL Generation Does not Show Description

Issue

WADL generation fails and a `java.lang.IllegalStateException: ServiceLocatorImpl` is returned.

```
Exception thrown when provider
class
org.glassfish.jersey.server.internal.monitoring.MonitoringFeature$Stati
sticsListener
was processing MonitoringStatistics. Removing provider from further
processing.
java.lang.IllegalStateException:
ServiceLocatorImpl(__HK2_Generated_6,9,221656053) has been shut down
at
org.jvnet.hk2.internal.ServiceLocatorImpl.checkState(ServiceLocatorImpl
.java:2393)
```

Also, when the WADL generation fails, the description field shows **Root Resource**, instead of a proper description in the following URLs.

```
http://<Host>:<AdminServerPort>/oam/services/rest/11.1.2.0.0/ssa/
policyadmin/application.wadl
http://<Host>:<ManagedServerPort>/iam/access/api/v1/health/
application.wadl
```

Resolution

Restart the Admin server and managed servers to resolve the wadl issue.

4.2 Troubleshooting Auto-Login Issues in an Access Manager and OIG Integrated Environment

The auto-login feature enables user login to Oracle Identity Governance after the successful completion of the Forgot Password or Forced Change Password flows, without prompting the user to authenticate using the new password.

Communication between Oracle Identity Governance and Access Manager can be configured to use Oracle Access Protocol (OAP) or TAP channels. Debugging auto-login issues is simplified if you determine which channel is being used. Determine the channel by examining the Oracle Identity Governance `SSOIntegrationMXBean` (version attribute) using the System MBean Browser in Oracle Enterprise Manager Fusion Middleware Control. For more information, see "Using the System MBean Browser" in *Administering Oracle Fusion Middleware*.

Depending upon the Access Manager version being used, the following applies:

- If the version is 11*g*, the TAP channel is used during auto-login. See Troubleshooting Oracle Access Protocol (OAP) Issues.

After a password is reset in Oracle Identity Governance and in LDAP through LDAP synchronization, Oracle Identity Governance redirects the user to the Access Manager TAP endpoint URL (`SSOIntegrationMXBean: TAPEndpointUrl`). Access Manager will auto-login the user by redirecting to the requested resource.

> **Note:**
>
> In the 12*c* Oracle Identity Governance and Access Manager integrated environment, the TAP protocol is configured for auto-login by default.

4.2.1 Troubleshooting TAP Protocol Issues

Check the OIG Server and Access Manager Server logs for any of the following error messages:

- 404 Not Found Error. For possible solution, see 404 Not Found Error
- System error. Please re-try your action. For possible solution, see System Error

4.2.1.1 404 Not Found Error

After resetting the password, user is redirected to a 404 Not Found error page.

Cause

The Access Manager TAP endpoint URL (`SSOIntegrationMXBean: TAPEndpointUrl)` is configured incorrectly.

Solution

Verify that `TAPEndpointUrl` is correctly configured in Oracle Identity Governance `SSOIntegrationMXBean` and is accessible. For example:

```
http://OAM_HOST:OAM_PORT/oam/server/dap/cred_submit
```

Or

```
http://OHS_HOST:OHS_PORT/oam/server/dap/cred_submit
```

where Access Manager is front-ended by OHS.

4.2.1.2 System Error

After resetting the password, user is redirected to Access Manager `TapEndpointUrl` (configured in Oracle Identity Governance `SSOIntegrationMXBean`), and the following error displays in the UI:

```
System error. Please re-try your action. If you continue to get this error, please
contact the Administrator.
```

Cause 1

A message similar to the following displays in the Access Manager Server logs:

```
Sep 19, 2012 4:29:45 PM EST> <Warning> <oracle.oam.engine.authn>

<BEA-000000> <DAP Token not received>

<Sep 19, 2012 4:29:45 PM EST> <Error> <oracle.oam.binding> <OAM-00002>

<Error occurred while handling the request.

java.lang.NullPointerException

at

oracle.security.am.engines.enginecontroller.token.DAPTokenEncIssuerImpl.issue(DAP
TokenEncIssuerImpl.java:87)
```

Solution 1

This error could be due to mis-configuration in `TAPResponseOnlyScheme` in Access Manager. Verify `oam-config.xml` (located at *`OAM_DOMAIN_HOME`*`/config/fmwconfig`) contains the following entry:

> **Note:**
>
> See Exporting and Importing the OAM Configuration File for the steps to export and import the `oam-config.xml` file.

```
<Setting Name="DAPModules" Type="htf:map">

     <Setting Name="7DASE52D" Type="htf:map">

         <Setting Name="MAPPERCLASS"
Type="xsd:string">oracle.security.am.engine.authn.internal.executor.DAPAttributeM
apper</Setting>

          <Setting Name="MatchLDAPAttribute" Type="xsd:string">uid</Setting>

          <Setting Name="name" Type="xsd:string">DAP</Setting>

     </Setting>

</Setting>
```

The value of `MatchLDAPAttribute` should be `uid`. If not, change the value.

To resolve the problem:

1. Login to Oracle Access Management Console.
2. Navigate to `TapResponseOnlyScheme`. Add the following as `Challenge` parameter:

   ```
   MatchLDAPAttribute=uid
   ```
3. Save the changes.

Cause 2

The following error displays in the Access Manager Server logs:

```
javax.crypto.BadPaddingException: Given final block not properly padded
```

This may occur if `OIM_TAP_PARTNER_KEY` is not include in the OIG credential map in the credential store, or if an invalid key is present.

Solution 2

Reregister Oracle Identity Governance as a TAP partner with Access Manager by rerunning the `OIGOAMIntegration.sh -configureSSOIntegration` option. and restart the complete OIG domain.

Cause 3

After resetting the password, if auto-login is not successful, the OIG server logs contain the following error:

```
Error occured while retrieving TAP partner key from Credential store
```

Solution 3

To resolve the problem:

1. Using Fusion Middleware Control, verify the `OIM_TAP_PARTNER_KEY` generic credential is present in the OIG credential map in the credential store.
2. If `OIM_TAP_PARTNER_KEY` is present, verify that LDAP connector is configured correctly, and that the password is reset in LDAP provider. Check this by issuing an `ldapbind` command with the user and the new/reset password.

Cause 4

After resetting the password, if auto-login is not successful, the OAM server logs have the following error:

```
Error occured while retrieving DAP token from OAM due to invalid TAP partner key
```

The `OIM_TAP_PARTNER_KEY` present in the OIG credential map of credential store is not valid.

Solution 4

Reregister Oracle Identity Management as a TAP partner with Access Manager by rerunning `OIGOAMIntegration.sh -configureSSOIntegration` option. You must restart the complete OIG domain.

Cause 5

After resetting the password, if auto-login is not successful, the OIG server logs may show the following error:

```
Error occurred when decrypting the DAP token
```

Solution 5

To resolve the problem, reset the TAP encryption key:

1. Update the `OIMPartner` attribute with `OIMPartnerOld` attribute by using OAM REST API. See Modifying OAM Configuration Parameters Using OAM REST API.
2. Delete `OIM_TAP_PARTNER_KEY` from the OIG domain using the Oracle Enterprise Manager Fusion Middleware Control.
3. Reregister Oracle Identity Governance as a TAP partner with Access Manager by rerunning the `OIGOAMIntegration.sh -configureSSOIntegration` option.

4. Verify that `OIM_TAP_PARTNER_KEY` is available in the domain credential store. See Validating the Oracle Identity Governance Domain Credential Store.
5. Restart OIG and OAM domain.

4.2.2 Troubleshooting Oracle Access Protocol (OAP) Issues

Check the OIG Server logs for any of the following types of error messages.

The resource URL is not protected.

Corrective action:

Verify that the correct `host:port` combination is configured in the Access Manager host identifier configuration.

1. Log in to the Oracle Access Management Console:

   `http://oam_adminserver_host:oam_adminserver_port/oamconsole`
2. In the Oracle Access Management Console, click **Application Security** at the top of the window.
3. Click **Host Identifiers** in the **Access Manager** section.
   The Search Host Identifiers page is displayed.
4. Click **Search** to initiate the search.
5. Click **IAMSuiteAgent** in the Search Results table.
6. Check the host identifiers for `host:port` combination in the identifier.
7. IAMSuiteAgent Host Identifier should have a combination of OHS (webserver) `host:port` which is front-ending Oracle Identity Management.

`aaaClient` is not initialized.

Corrective action:

Verify that the passwords seeded into OIG domain credential store are correct. For `OPEN` mode, check for the WebGate password. For `SIMPLE` mode, check that SSO keystore password and SSO global passphrase are seeded in correctly. For more information, see Validating the Oracle Identity Governance Domain Credential Store.

Failed to communicate with any of configured OAM Server.

Corrective action:

- Verify that it is up and running.
- Verify that the passwords seeded into OIG domain credential store are correct.
- For OPEN mode, check for the WebGate password.
- For SIMPLE mode, check that SSO keystore password and SSO global passphrase also are seeded in correctly.

See Validating the Oracle Identity Governance Domain Credential Store.

`SSOKeystore` tampered or password is incorrect.

Corrective action:

- Check that the keystore file `ssoKeystore.jks` is present in *`OIM_DOMAIN_HOME`*`/config/fmwconfig`.
- If present, then check if the keystore password is seeded properly into OIG domain credential store.

See Validating the Oracle Identity Governance Domain Credential Store.

Oracle Identity Management logs do not have any information about the failure.

Corrective action:

- Enable HTTP headers and capture the headers while running through the First Login, Forgot Password flows. See Diagnosing Single Sign-On Issues By Capturing HTTP Headers.
- In the HTTP headers, look for `Set-Cookie: ObSSOCookie` after the POST method on the First Login, Forgot Password page. Check the domain of the cookie. It should match with the domain for the protected resource URL.
- If cookie domain is different, update the `CookieDomain` in the Oracle Identity Management SSO configuration using Fusion Middleware Control. See Validating the Oracle Identity Governance SSO Configuration Settings.
- If cookie domain is correct, then check for any time differences on the machines which host the OIG and OAM Servers.

4.3 Troubleshooting Session Termination Issues

The session termination feature enables the termination of all active user sessions after the user status is modified by an Oracle Identity Management administrator. The following Oracle Identity Management operations lead to session termination: user lock, disable or delete.

To troubleshoot session termination issues:

- Verify the OAM REST URL, http://<OAM_HOST>:<OAM_PORT>/oam/services/rest/access/api/v1/session?userId=<uid>is accessible.

  Here, OAM_HOST refers to `SSOIntegrationMXBean: AccessServerHost` and OAM_PORT refers to `SSOIntegrationMXBean: OAMServerPort`
- Verify if OAM Admin has authorization to invoke OAM REST API (`SSOIntegrationMXBean: OAMAdminUser`).
- Verify in `oam-config.xml` in OAM domain that `UserStore` in `SessionRuntime` points to `IDStore` created during integration.
- Verify `/db/sssointg/EventHandlers.xml` is in Oracle Identity Governance MDS. See Validating the Oracle Identity Governance Event Handlers Configured for SSO.

4.4 Troubleshooting Account Self-Locking Issues

Use Case 1

Both LDAP store and Access Manager lock out the user due to multiple failed login attempts. The user attempts to reset his or her password using the Oracle Identity Governance (OIG) "Forgot Password" page, but the reset operation fails.

Possible explanation: the user's locked status has not yet propagated to Oracle Identity Governance.

1. Check if the user is locked in Oracle Identity Governance:
    a. Log in to the Identity Self Service application as an Oracle Identity Governance administrator.
    b. Navigate to the **Users** section, then search for the user.
    c. Check if the Identity status is `locked`.
2. If the status is not `locked`, run a **SSO User Incremental Reconciliation** scheduled job, and then confirm that the user status is `locked`.

Use Case 2

The user account self-locks due to multiple invalid credentials login attempts. Later, when the user attempts to log in with the correct credentials, he or she is not able to log in. The user expects to log in first and then change the password, but login fails consistently.

Possible explanation: both LDAP directory and Access Manager may have locked the user account. In this case the user cannot log in to Oracle Identity Governance or to any protected page. The user has to use the Forgot Password flow to reset the password.

Note that if only Access Manager locks out the user, the user can log in to Oracle Identity Governance and change the password immediately.

Use Case 3

The LDAP directory `pwdMaxFailure` count of three is less than the `oblogintrycount` value of five. The LDAP directory locks out the user due to multiple invalid credentials login attempts (in this case, three attempts). Later, when the user tries to log in with the correct credentials, on the fourth attempt the user still cannot log in. The user expects to log in first and then change the password, but login fails consistently.

Possible explanation: LDAP directory locked out the user, but Access Manager did not. The user cannot log in with the correct password even though the `oblogintrycount` is less than five, but following the Forgot Password flow works and resets the password.

Note that when LDAP directory locks out the user there is nothing to reconcile into OIG, because OIG does not reconcile user accounts that are locked in LDAP store. When LDAP store locks the user, OIG shows the user as active. Following the Forgot Password flow is the only way to reset the password.

Use Case 4

The LDAP directory `pwdMaxFailure` count value of seven is less than the `oblogintrycount` value of five. Access Manager locked out the user due to multiple invalid credentials login attempts. Later, when the user tries to login with the correct credentials, the user is able to log in and is redirected to change the password, but the reset password operation fails.

Possible explanation: the user locked status has not yet propagated to OIG.

1. Check if the user is locked in OIG:
    a. Login to Identity Self Service application as an OIG administrator.

b. Navigate to **Users** section, then search for the user.

c. Check if the Identity status is `locked`.

2. If the status is not `locked`, run a **SSO User Incremental Reconciliation** scheduled job, and then confirm that the user status is `locked`.

Note that use case one and this use case look similar. In use case one, both LDAP directory and Access Manager locked the user account, whereas in this use case only Access Manager locks the user. The remedy for both use cases is the same, however.

Use Case 5

The user cannot remember his or her password and tries to reset the password using the Forgot Password flow. The user provides his or her user login, provides a new password, and provides incorrect challenge answers. After three failure attempts, both LDAP directory and Access Manager lock the user. The user expects to get locked out after five attempts instead of three attempts because the `oblogintrycount` value is 5.

Possible explanation: the password reset attempts in the OIG Reset/Forgot Password flow are governed by the OIG system property `XL.MaxPasswordResetAttempts` and the default value is 3. Consequently, the user is locked out immediately after three attempts. OIG locks the user natively in LDAP directory and in Access Manager.

Note that password reset attempts are different from login attempts. Login attempts are governed by Access Manager (`oblogintrycount=5`) and password reset attempts by OIG (`XL.MaxPasswordResetAttempts=3`).

Use Case 6

LDAP directory locks the user because some constant LDAP binding used incorrect credentials. Access Manager does not lock out the user. When the user tries to log in with the correct credentials, he is not able to log in.

Possible explanation: LDAP directory locks the user out in this use case, not Access Manager. The user cannot log in with the correct password even if the `oblogintrycount` is still less than 5, but the user can reset his or her password by following the Forgot Password flow.

Note that when a user is only locked out by LDAP directory, the user's lock-out status is not reconciled into OIG. Consequently, the user shows up as still active in OIG even though the user is locked in LDAP directory.

Use Case 7

When the user resets his password, the password reset is not immediate.

1. The user account self-locks due to multiple invalid credentials login attempts.
2. The user uses the Forgot Password flow to reset the password.
3. The user account is still locked, and he is not able to login to Oracle Identity Governance.

Possible explanation: the user's `locked` status has not yet propagated to OIG.

1. Check if the user is locked in OIG:

   a. Login to Identity Self service application as an OIG administrator.

   b. Navigate to the **Users** section, and then search for the user.

   c. Check if the Identity status is `locked`.

2. If the status is not `locked`, run an **SSO User Incremental Reconciliation** scheduled job, and then confirm that the user status is `locked`.

4.5 Troubleshooting Miscellaneous Issues in an Access Manager and OIG Integrated Environment

This provides solutions for the following miscellaneous issues:

- Scheduler and System Properties do not come up in the Integrated Environment
- Client Based Oracle Identity Governance Login Failure
- Logout 404 Error Occurs After Logging Out of OIG protected Application
- Old Password Remains Active After Password Reset
- OIG Configuration Failure During Seeding of OIG Policies into Access Manager
- Adding Object Classes Fails
- SSO Reconciliation Filter Does Not Work With DN Attributes for Trusted Source Reconciliation
- Login Fails for Users Created Through Bulk Load
- Events are Generated Without Any Changes in the Target

4.5.1 Scheduler and System Properties do not come up in the Integrated Environment

When accessing the scheduler page, the following error occurs and configuration properties are not visible.

```
Failed <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <html><head>
<title>404 Not Found</title> </head><body> <h1>Not Found</h1> <p>The
requested URL /iam/governance/selfservice/api/v1/scheduler/history was
not
found on this server.</p> </body></html>
```

Solution

1. Add the following entries in the `oim.conf` file at the following locations:
   Locations:

   ```
   OAM_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf/
   oim.conf
   ```

   ```
   OAM_DOMAIN_HOME/config/fmwconfig/components/OHS/instances/ohs1/
   moduleconf/oim.conf
   ```

   Entries

   ```
   <Location /iam/governance/adminservice/api/v1>
    SetHandler weblogic-handler
   ```

```
 WLCookieName oimjsessionid
 WebLogicHost %OIM_HOST%
 WebLogicPort %OIM_PORT%
 WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>


<Location /iam/governance/selfservice/api/v1>
 SetHandler weblogic-handler
 WLCookieName oimjsessionid
 WebLogicHost %OIM_HOST%
 WebLogicPort %OIM_PORT%
 WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>
```

2. Restart the servers

4.5.2 Client Based Oracle Identity Governance Login Failure

For successful client-based login to Oracle Identity Governance:

- The client-based login user must be present in the LDAP provider.
- An LDAP Authenticator must be configured in the OIG domain security realm corresponding to the LDAP provider where the user is present. See Validating the Oracle Identity Governance Security Provider Configuration.

4.5.3 Logout 404 Error Occurs After Logging Out of OIG protected Application

If logging out of an Oracle Identity Governance protected application throws a `404` error, verify that the logout configuration is present in `jps-config.xml`. See Validating the Oracle Identity Governance SSO Logout Configuration.

If needed, the JPS configuration can be fixed by editing the `jps-configuration` file located in *`$DOMAIN_HOME`*`/config/fmwconfig` and then restarting all the servers.

To resolve a misconfiguration in `jps-config.xml`:

1. In a terminal window issue the following commands: `cd $$ORACLE_HOME <OIG_INSTALL_LOCATION>/oracle_common/common/bin`
2. `./wlst.sh`
3. `connect()`
4. `addOAMSSOProvider(loginuri="/${app.context}/adfAuthentication", logouturi="/oamsso/logout.html", autologinuri="/obrar.cgi")`
5. `exit`
6. Restart all servers in the domain.

   See Starting and Stopping Admin Server in *Administering Oracle Fusion Middleware*

4.5.4 Old Password Remains Active After Password Reset

In Active Directory environments, old passwords can remain active for up to one hour after a password reset. During this interval, both the old and new password can successfully bind to the Active Directory server. This is the expected behavior.

4.5.5 OIG Configuration Failure During Seeding of OIG Policies into Access Manager

As part of running `OIGOAMIntegration.sh -configureSSOIntegration`, Oracle Identity Governance policies are seeded into Access Manager using the Access Management exposed REST endpoint.

An exception while seeding Oracle Identity Governance policies occurs when the user credentials used for accessing Access Manager exposed endpoint does not have enough privileges to perform the operation.

The solution is as follows:

1. Make sure `IDSTORE_WLSADMINUSER` is the same user which was used while running the `prepareIdStore mode=wls` command.
2. Try to access the Access Manager REST endpoint using `curl` command:

   ```
   curl -u weblogic_idm:password "http://OAM_ADMIN_HOST:OAM_ADMIN_PORT/oam/
   services/rest/11.1.2.0.0/ssa/policyadmin/appdomain"
   ```

   Where:

   - `weblogic_idm` is the user as mentioned for `IDSTORE_WLSADMINUSER` and *`password`* is the password for the user.

   If this command fails to return the list of application domains present in Access Manager, then make sure `configOAM` is run properly and the Access Manager admin server is restarted before running `OIGOAMIntegration.sh -configureSSOIntegration`.

4.5.6 Adding Object Classes Fails

When you run the `OIGOAMIntegration.sh -addMissingObjectClasses` to add the object class. It fails with the following error:

```
ldap_bind: Invalid credentials (49)
```

Cause

This error occurs when you provide additional space for the `IDSTORE_BINDDN` property in the `addMissingObjectClasses.config` file.

Example

```
IDSTORE_BINDDN:cn=Directory Manager
```

Solution

1. Ensure that you provide the double quotation marks (") at the beginning and end for the `IDSTORE_BINDDN` property.
   Example

   ```
   IDSTORE_BINDDN:cn="Directory Manager"
   ```

2. Replace the following lines from the `addMissingObjectClasses` function in the `_OIGOAMIntegration.sh` script:

   ```
   COMMAND="ldapsearch -h $IDSTORE_HOST -p $IDSTORE_PORT -D $IDSTORE_BINDDN -
   w $IDSTORE_BINDDN_PWD -b $IDSTORE_USERSEARCHBASE -s sub $FILTER dn"
   echo "Executing ldapsearch..."
   echo $COMMAND
   $COMMAND | grep "dn:" > ${ALL_USERS}
   ```

   With the following lines:

   ```
   LDAP_COMMAND="ldapsearch -h $IDSTORE_HOST -p $IDSTORE_PORT -D
   "$IDSTORE_BINDDN" -w $IDSTORE_BINDDN_PWD -b $IDSTORE_USERSEARCHBASE -s
   sub $FILTER dn"
   COMMAND=$(ldapsearch -h $IDSTORE_HOST -p $IDSTORE_PORT -D
   "$IDSTORE_BINDDN" -w $IDSTORE_BINDDN_PWD -b $IDSTORE_USERSEARCHBASE -s
   sub $FILTER dn)
   echo "Executing ldapsearch..."
   echo $LDAP_COMMAND
   echo $COMMAND | grep "dn:" > ${ALL_USERS}
   ```

4.5.7 SSO Reconciliation Filter Does Not Work With DN Attributes for Trusted Source Reconciliation

When you use `Contains`, `startsWith`, and `endsWith` filters with the `entryDN` field, SSO full and incremental reconciliation fails with the following error:

```
org.identityconnectors.framework.common.exceptions.ConnectorException:
Unsupported filter type for attribute entryDN
```

The LDAP filters on the `entryDN` and `DN` attributes are not supported as per the LDAP connector specification/implementation. Only the `__parentDN__` attribute with the `equalTo` filter is supported as per the current LDAP filter support. Therefore, for fetching users under the OU as part of trusted reconciliation, the `equalTo` filter must be applied on the `__parentDN__` attribute.

4.5.8 Login Fails for Users Created Through Bulk Load

In an OAM-OIG integrated environment with AD used as LDAP in connector-based setup, if login does not work for users created through bulk load, then follow the solution described in this topic.

Cause

This happens because in the AD target user attribute `sAMAccountName` has some junk value, such as `$JI7000-BD7NAT1841M6`, instead of the actual user ID.

Solution

When AD is used as LDAP, update the transformation script for the application `SSOTarget` to add the condition for `BULKLOAD`. To do so:

1. Login to Oracle Identity Self Service.
2. Click the **Manage** tab, and edit the `SSOTarget` application from the Applications page.
3. Go to the Settings page, and click the **Reconciliation** tab.
4. In the Validation & Transformation section, click **Transformation Script** to open the editor.
5. Add the condition for `BULKLOAD`, as shown:

```
(context.provisionMechanism.equalsIgnoreCase("REQUEST")
||
context.provisionMechanism.equalsIgnoreCase("ADMIN")
||
context.provisionMechanism.equalsIgnoreCase("BULKLOAD")
)
{
if (User_Id == null || User_Id == "") {
User_Id = getBeneficiaryAttrFromContext("User Login");
}
```

6. Save the changes.

After adding this condition for `BULKLOAD`, reload all the bulkload users, and then attempt for login.

4.5.9 Events are Generated Without Any Changes in the Target

When you run the SSO User Incremental Reconciliation scheduled job, events are generated although there are no changes done in the target.

Cause

Events are generated because the `obPasswordExpiryDate` field value coming from the target is not formatted correctly in OIG.

Solution

1. In Oracle Identity Self Service, click the **Manage** tab, and edit the `SSOTarget` application from the Applicaitons page.
2. Go to the Schema page and change the advanced settings of the `obPasswordExpiryDate` schema attribute to enable the **Date** option.
3. Save the changes.
4. Run the SSO User Incremental Reconciliation scheduled job.

4.6 Troubleshooting Target Account Creation

The target account creation may fail due to some known reasons. This section helps you troubleshoot and solve some known issues while creating a target account and resetting password in OUD.

Container rules are not configured in SSOIntegrationMXBean

Corrective action:

- Execute `addContainerRules` operation manually against `SSOIntegrationMXBean`.
- Or update the appropriate configuration file and run one of the following scripts:
  - $ORACLE_HOME/idm/server/ssointg/bin/OIGOAMIntegration.sh -configureLDAPConnector
  - $ORACLE_HOME/idm/server/ssointg/bin/OIGOAMIntegration.sh -updateContainerRules

Application Instance is not created

Corrective action:

- Create the Application Instance manually. For more information, see Creating Target Application Instance.
- Or update the appropriate configuration file and run the following script:

```
$ORACLE_HOME/idm/server/ssointg/bin/OIGOAMIntegration.sh -configureLDAPConnector
```

LDAP server is not running

Corrective action: Start the LDAP server

Directory is not seeded

Corrective action:

Update the appropriate configuration file and run the following script:

```
$ORACLE_HOME/idm/server/ssointg/bin/OIGOAMIntegration.sh -prepareIDStore
```

mds-oim connection pool is unable to allocate another connection

Corrective action:

- From the WebLogic console, navigate to **Services>Data Sources>mds-oim>Connection Pool**.
- On the **Connection Pool** page, increase the values of **Initial Capacity**, **Minimum Capacity**, and **Maximum Capacity**.
- Click **Save**.
- On the **Connection Pool** page, select **Advanced** link available at the bottom of the page.
- On the **Advanced** page, set the value of `Inactive Connection Timeout` to a non-zero value, for example `10`.
- Click **Save**

Resetting password in OUD

When the System Administrator manually locks a user in OIG, the attributes `obLockedOn` and `pwdAccountLockedTime` are set for the user in OUD. If the System Administrator resets the user's password, `pwdAccoundLockedTime` is cleared in the OUD. This is a default behavior in OUD.

When the `pwdAccoundLockedTime` attribute is cleared, the user status gets updated to unlocked after user reconciliation in OIG. However, `obLockedOn` is still set in OUD and OAM treats this user as locked.

Corrective action:

It is recommended to lock (or unlock) the user from OIG. This scenario is applicable only to reset password for a manually locked-user. It does not apply to change password for self-locked user where user is locked due to failed password attempts.

4.7 Troubleshooting prepareIDStore for AD

Error

Schema in `ADUserSchema.ldif` fails to load.

This error appears when running the following script step.

```
oracle.ldap.util.LDIFLoader loadOneLdifFile INFO: Ignoring Error:
javax.naming.directory.InvalidAttributeValueException: [LDAP: error code 19 -
00002082: AtrErr: DSID-03151817, #1: 0: 00002082: DSID-03151817, problem 1005
(CONSTRAINT_ATT_TYPE), data 0, Att90094 (schemaIDGUID):len 26 ]; remaining name
'cn=oblocationdn,cn=schema,cn=configuration,DC=interop55,DC=us,DC=oracle,DC=com'
```

Solution

1. Edit `ADUserSchema.ldif` and replace `%IDSTORE_SEARCHBASE%` with `DC=interop55,DC=my,DC=org,DC=com`
2. Run the LDAP command to load them into AD

   ```
   ldapmodify -h 192.0.2.1 -p 389 -D Administrator@interop -w <password> -f
   ADUserSchema.ldif -c -x
   ```

Problem

In AD environment, the object classes such as `oblixgroup` are not loaded after `prepareIDStore` step is run.

Solution

1. Navigate to `$ORACLE_HOME/idm/server/ldif/prepareidstore/AD/schema`
2. Edit `ADUserSchema.ldif` and replace `%IDSTORE_SEARCHBASE%` with the location in the directory where users and groups are stored. For example, dc=example,dc=com

   .

3. Run the LDAP command

```
ldapmodify -h <activedirectoryhostname> -p <activedirectoryportnumber> -D
<AD_administrator> -f ADUserSchema.ldif -w <password> -c -x
```

where `AD_administrator` is the user with schema extension privileges to the directory.

Example:

```
ldapmodify -h activedirectoryhost.example.com -p 389 -D adminuser -f
ADUserSchema.ldif -w password -c -x
```

4.8 Troubleshooting the OIG-OAM Integrated Environment Upgrade

After upgrading from an 11.1.2.3.0 environment to 12.2.1.4.0, when you perform the First Login flow, or Forgot Password Flow, or Reset Password Flow then auto-login fails and system error message appears. When you initiate above flows, new password and challenge questions are set correctly irrespective of the system error.

To resolve this issue, you must re-login with the newly set password.

5

Modifying OAM Configuration Properties

You can change OAM configuration by modifying the oam-config.xml file or by modifying OAM configuration properties using OAM REST API.

Topics include:

- Exporting and Importing the OAM Configuration File
- Modifying OAM Configuration Parameters Using OAM REST API

5.1 Exporting and Importing the OAM Configuration File

To modify the `oam-config.xml` file, export the file from the database, update it, and then import it back to the database.

To update the `oam-config.xml` file in UNIX/Linux environment:

1. Set the following environment variables for Oracle Access Manager:
   - `ORACLE_HOME`
   - `DOMAIN_HOME`
   - `JAVA_HOME`
   - `DB_ORACLE_HOME`
2. Create the `prop.properties` file.

   The following shows an example of the `prop.properties` file.

   ```
   oam.entityStore.ConnectString=jdbc:oracle:thin:@dbhost.example.com:1521/
   servicename.example.com
   oam.entityStore.schemaUser=MYPREFIX_OAM
   oam.entityStore.schemaPassword=xxxxx
   oam.importExportDirPath=/tmp
   oam.frontending=params=oamhost.example.com;14100;http
   ```
3. Export `oam-config.xml` located in the *`DOMAIN_HOME`*`/config/fmwconfig/` directory into temporary location (`tmp`) by running the following command:

   ```
   java -cp config-utility.jar:ojdbc8.jar
   oracle.security.am.migrate.main.ConfigCommand <path to which configuration must be
   exported> export <prop.properties>
   ```

   For example:

   ```
   $JAVA_HOME/bin/java -cp $ORACLE_HOME/idm/oam/server/tools/config-utility/config-
   utility.jar:$DB_ORACLE_HOME/jdbc/lib/ojdbc8.jar
   oracle.security.am.migrate.main.ConfigCommand $DOMAIN_HOME export /tmp/
   prop.properties
   ```
4. Open the `oam-config.xml` file under `temp` folder in a text editor and update the required attribute.
5. Import `oam-config.xml` into the database by running the following command:

```
java -cp config-utility.jar:ojdbc8.jar
oracle.security.am.migrate.main.ConfigCommand <path to which configuration
must be exported> import <prop.properties>
```

For example:

```
$JAVA_HOME/bin/java -cp $ORACLE_HOME/idm/oam/server/tools/config-utility/
config-utility.jar:$DB_ORACLE_HOME/jdbc/lib/ojdbc8.jar
oracle.security.am.migrate.main.ConfigCommand $DOMAIN_HOME import /tmp/
prop.properties
```

To update the `oam-config.xml` file in Windows environment:

a. Navigate to <OS_DRIVE>\Users\<USERNAME>\<Documents>
Here, <USERNAME> is the username of the logged-in user.

b. Create the prop.properties file with the following entries:

```
oam.entityStore.ConnectString=jdbc:oracle:thin:@<DB_HOSTNAME>:<DB_PORT></
SERVICE_NAME>
oam.entityStore.schemaUser=<OAM_SCHEMA_NAME>
oam.entityStore.schemaPassword=<OAM_SCHEMA_PASSWORD>
oam.importExportDirPath=<DIRECTORY_PATH>
oam.frontending=params=WebLogicHost:OAMManagedServerPort:http(s)
```

c. Copy config-utility.jar and ojdbc8.jar to
<OS_DRIVE>\Users\<USERNAME>\Documents>.

d. Set JAVA_HOME=<1.8.0_131_JDK_OR_HIGHER>

e. Open the command prompt and navigate as shown:

```
cd <OS_DRIVE>\Users\<USERNAME>\Documents>
```

f. Run the following commands for export and import:
For export:

```
java -cp ".;config-utility.jar;ojdbc8.jar"
oracle.security.am.migrate.main.ConfigCommand\<MIDDLEWARE_HOME>\user_proj
ects\domains\<OAM_DOMAIN> export prop.properties
```

For import:

```
java -cp ".;config-utility.jar;ojdbc8.jar"
oracle.security.am.migrate.main.ConfigCommand\<MIDDLEWARE_HOME>\user_proj
ects\domains\<OAM_DOMAIN> import prop.properties
```

5.2 Modifying OAM Configuration Parameters Using OAM REST API

To modify OAM configuration parameters by using OAM REST API:

1. Edit the oamconfig_modify.xml file, change the OAM parameters. The following is a sample:

```
<Configuration>
<Setting Name="host" Type="xsd:string" Path="/DeployedComponent/
Server/NGAMServer/Instance/oam_server1/host">@OAM_SERVER@1</Setting>
<Setting Name="host" Type="xsd:string" Path="/DeployedComponent/
Server/NGAMServer/Instance/oam_server2/host">@OAM_SERVER@2</Setting>
```

```
<Setting Name="Port" Type="xsd:integer" Path="/DeployedComponent/Server/
NGAMServer/Instance/oam_server1/oamproxy/Port">@OAP_PORT@</Setting>
<Setting Name="Port" Type="xsd:integer" Path="/DeployedComponent/Server/
NGAMServer/Instance/oam_server2/oamproxy/Port">@OAP_PORT@</Setting>
<Setting Name="serverhost" Type="xsd:string" Path="/DeployedComponent/
Server/NGAMServer/Profile/OAMServerProfile/OAMSERVER/
serverhost">@LBR_HOST@</Setting>
<Setting Name="serverport" Type="xsd:string" Path="/DeployedComponent/
Server/NGAMServer/Profile/OAMServerProfile/OAMSERVER/
serverport">@LBR_PORT@</Setting>
<Setting Name="serverprotocol" Type="xsd:string" Path="/DeployedComponent/
Server/NGAMServer/Profile/OAMServerProfile/OAMSERVER/
serverprotocol">@LBR_PROTOCOL@</Setting>
<Setting Name="serverhost" Type="xsd:string" Path="/DeployedComponent/
Server/NGAMServer/Profile/OAMServerProfile/OAMServerBackChannel/
serverhost">@LBR_HOST@</Setting>
<Setting Name="serverport" Type="xsd:string" Path="/DeployedComponent/
Server/NGAMServer/Profile/OAMServerProfile/OAMServerBackChannel/
serverport">@LBR_PORT@</Setting>
<Setting Name="serverprotocol" Type="xsd:string" Path="/DeployedComponent/
Server/NGAMServer/Profile/OAMServerProfile/OAMServerBackChannel/
serverprotocol">@LBR_PROTOCOL@</Setting>
<Setting Name="OAMRestEndPointHostName" Type="xsd:string" Path="/
DeployedComponent/Agent/WebGate/Instance/accessgate-oic/
UserDefinedParameters/OAMRestEndPointHostName">@LBR_HOST@</Setting>
<Setting Name="OAMRestEndPointPort" Type="xsd:string" Path="/
DeployedComponent/Agent/WebGate/Instance/accessgate-oic/
UserDefinedParameters/OAMRestEndPointPort">@LBR_PORT@</Setting>
<Setting Name="providerid" Type="xsd:string" Path="/DeployedComponent/
Server/NGAMServer/Profile/STS/fedserverconfig/
providerid">@LBR_PROTOCOL@://@LBR_HOST@:@LBR_PORT@/oam/fed</Setting>
<Setting Name="Value" Type="xsd:string" Path="/DeployedComponent/Server/
NGAMServer/Instance/oam_server1/CoherenceConfiguration/LocalHost/
Value">@OAM_SERVER@1</Setting>
<Setting Name="Value" Type="xsd:string" Path="/DeployedComponent/Server/
NGAMServer/Instance/oam_server2/CoherenceConfiguration/LocalHost/
Value">@OAM_SERVER@2</Setting>
<Setting Name="assertionissuer" Type="xsd:string" Path="/
DeployedComponent/Server/NGAMServer/Profile/STS/issuancetemplates/saml11-
issuance-template/assertionissuer">@LBR_HOST@</Setting>
<Setting Name="assertionissuer" Type="xsd:string" Path="/
DeployedComponent/Server/NGAMServer/Profile/STS/issuancetemplates/saml20-
issuance-template/assertionissuer">@LBR_HOST@</Setting>
<Setting Name="openid20realm" Type="xsd:string" Path="/DeployedComponent/
Server/NGAMServer/Profile/STS/spglobal/openid20realm">@LBR_PROTOCOL@://
@LBR_HOST@:@LBR_PORT@</Setting>
<Setting Name="logoutRedirectUrl" Type="xsd:string" Path="/
DeployedComponent/Agent/WebGate/Instance/accessgate-oic/
logoutRedirectUrl">@LBR_PROTOCOL@://@LBR_HOST@:@LBR_PORT@/oam/server/
logout</Setting>
<Setting Name="security" Type="xsd:string" Path="/DeployedComponent/Agent/
WebGate/Instance/accessgate-oic/security">simple</Setting>
<Setting Name="security" Type="xsd:string" Path="/DeployedComponent/Agent/
WebGate/Instance/IAMSuiteAgent/security">simple</Setting>
<Setting Name="logoutRedirectUrl" Type="xsd:string" Path="/
```

```
DeployedComponent/Agent/WebGate/Instance/IAMSuiteAgent/
UserDefinedParameters/logoutRedirectUrl">@LBR_PROTOCOL@://
@LBR_HOST@:@LBR_PORT@/oam/server/logout</Setting>
<Setting Name="Timeout" Type="htf:timeInterval" Path="/
DeployedComponent/Server/NGAMServer/Profile/Sme/
SessionConfigurations/Timeout">15 M</Setting>

<Setting Name="PrimaryServerList" Type="htf:list" Path="/
DeployedComponent/Agent/WebGate/Instance/IAMSuiteAgent/
PrimaryServerList">
<Setting Name="0" Type="htf:map" Path="/DeployedComponent/Agent/
WebGate/Instance/IAMSuiteAgent/PrimaryServerList/0">
<Setting Name="host" Type="xsd:string" Path="/DeployedComponent/
Agent/WebGate/Instance/accessgate-oic/PrimaryServerList/0/
host">@OAP_HOST@</Setting>
<Setting Name="port" Type="xsd:string" Path="/DeployedComponent/
Agent/WebGate/Instance/accessgate-oic/PrimaryServerList/0/
port">@OAP_SERVICEPORT@</Setting>
<Setting Name="numOfConnections" Type="xsd:string" Path="/
DeployedComponent/Agent/WebGate/Instance/accessgate-oic/
PrimaryServerList/0/numOfConnections">20</Setting>
</Setting>
</Setting>

<Setting Name="PrimaryServerList" Type="htf:list" Path="/
DeployedComponent/Agent/WebGate/Instance/accessgate-oic/
PrimaryServerList">
<Setting Name="0" Type="htf:map" Path="/DeployedComponent/Agent/
WebGate/Instance/accessgate-oic/PrimaryServerList/0">
<Setting Name="port" Type="xsd:string" Path="/DeployedComponent/
Agent/WebGate/Instance/accessgate-oic/PrimaryServerList/0/
port">@OAP_SERVICEPORT@</Setting>
<Setting Name="numOfConnections" Type="xsd:string" Path="/
DeployedComponent/Agent/WebGate/Instance/accessgate-oic/
PrimaryServerList/0/numOfConnections">20</Setting>
<Setting Name="host" Type="xsd:string" Path="/DeployedComponent/
Agent/WebGate/Instance/accessgate-oic/PrimaryServerList/0/
host">@OAP_HOST@</Setting>
</Setting>
</Setting>
</Configuration>
```

2. Run the following cURL command:

```
curl -x '' -X PUT $ADMIN_PROTOCOL://$ADMIN_HOST:$ADMIN_PORT/iam/admin/
config/api/v1/config -ikL -H 'Content-Type: application/xml' --user $user -H
'cache-control: no-cache' -d @$cur_dir/output/oamconfig_modify.xml
```

Part III
External SSO Solutions

You can integrate federation partners into the Oracle IdM environment.

This part contains the following chapter:

- Integrating with Identity Federation

6
Integrating with Identity Federation

This chapter explains how Oracle Access Management Access Manager leverages identity federation to create an authenticated session with a federation partner.
This chapter contains these sections:

- Introduction to Identity Federation with Oracle Access Manager
- Integrating Access Manager 11gR2 with Identity Federation 11gR1
- Running Access Manager-OIF Integration Scripts to Automate Tasks

6.1 Introduction to Identity Federation with Oracle Access Manager

This section provides background about federation with Access Manager.

Topics include:

- About Oracle Access Management Identity Federation
- About Deployment Options for Identity Federation

6.1.1 About Oracle Access Management Identity Federation

Identity federation is available in two architectures:

- As a federation engine, known as Oracle Access Management Identity Federation, built into Oracle Access Management (11g Release 2 (11.1.2).
- As a standalone, self-contained federation server, known as Oracle Identity Federation, that enables single sign-on and authentication in a multiple-domain identity network (11g Release 1 (11.1.1).

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

6.1.2 About Deployment Options for Identity Federation

> **See Also:**
>
> For details about naming conventions and name changes in Oracle Access Management, see *Introduction to Oracle Access Management* in *Administering Oracle Access Management*.

Various deployment options are available for leveraging identity federation with Access Manager to create an authenticated user session.

The Oracle Fusion Middleware framework supports these integrated approaches to cross-domain single sign-on:

- An Oracle Access Management Identity Federation engine built into the Access Manager server. All configuration is performed in Access Manager.

  This approach is available in 12*c* (12.2.2). The engine supports both Service Provider (SP) and Identity Provider (IdP) modes.

- Separate Oracle Identity Federation and Oracle Access Manager servers that can be integrated to provide federation capabilities. Management and configuration of both servers is required for this integration.

  This approach is available in 11*g* Release 1 (11.1.1).

  Under this approach, Oracle Identity Federation provides two deployment scenarios for Oracle Access Manager:

  – Oracle Identity Federation 11*g* Release 1 (11.1.1) integrated with Oracle Access Manager 10*g*

  – Oracle Identity Federation 11*g* Release 1 (11.1.1) integrated with Access Manager 11*g*

Table 6-1 summarizes the options available to integrate the identity federation products with Oracle Access Management Access Manager and provides links to deployment procedures:

Table 6-1 Deployment Options involving Oracle Access Manager 10g and Access Manager 11g

Access Manager Version	Description	Additional Information
Oracle Access Management Access Manager 11*g*R2	Access Manager contains a built-in federation engine that supports both SP and IdP mode functionality configurable through the Oracle Access Management Console.	Introduction to Federation within Oracle Access Suite Console in *Administering Oracle Access Management* Integrating Access Manager 11gR2 with Identity Federation 11gR1
Oracle Access Manager 11*g*R1	The stand-alone Oracle Identity Federation 11g Release 1 server integrates with the Access Manager 11*g* server.	Integrating Oracle Identity Federation in *Integration Guide for Oracle Access Manager*.
Oracle Access Manager 10*g*	The stand-alone Oracle Identity Federation 11g Release 1 server integrates with the Oracle Access Manager 10*g* server.	Deploying Oracle Identity Federation with Oracle Access Manager 10g in *Administrator's Guide for Oracle Identity Federation*.

6.1.3 References

Introduction to Oracle Identity Federation in *Administrator's Guide for Oracle Identity Federation*.

6.2 Integrating Access Manager 11gR2 with Identity Federation 11gR1

This section describes how to integrate Access Manager 12*c* (12.2.2) with Oracle Identity Federation 11*g* Release 1 (11.1.1).

This is also referred to as Access Manager 11*g*R2 with Oracle Identity Federation 11*g*R1.

- About SP and Authentication Integration Modes
- Access Manager and Oracle Identity Federation Integration Overview
- Prerequisites to Integrating Access Manager with Oracle Identity Federation
- Verifying Servers are Running and a Resource is Protected
- Registering Oracle HTTP Server WebGate with Access Manager for Access Manager and OIF Integration
- Configuring Oracle Identity Federation for Access Manager and OIF Integration
- Configuring Access Manager for Integration with Oracle Identity Federation
- Configuring Access Manager to Protect a Resource with the OIFScheme
- Testing the Access Manager and Oracle Identity Federation Integration Configuration

6.2.1 About SP and Authentication Integration Modes

Two integration modes are described in this chapter:

- SP Mode

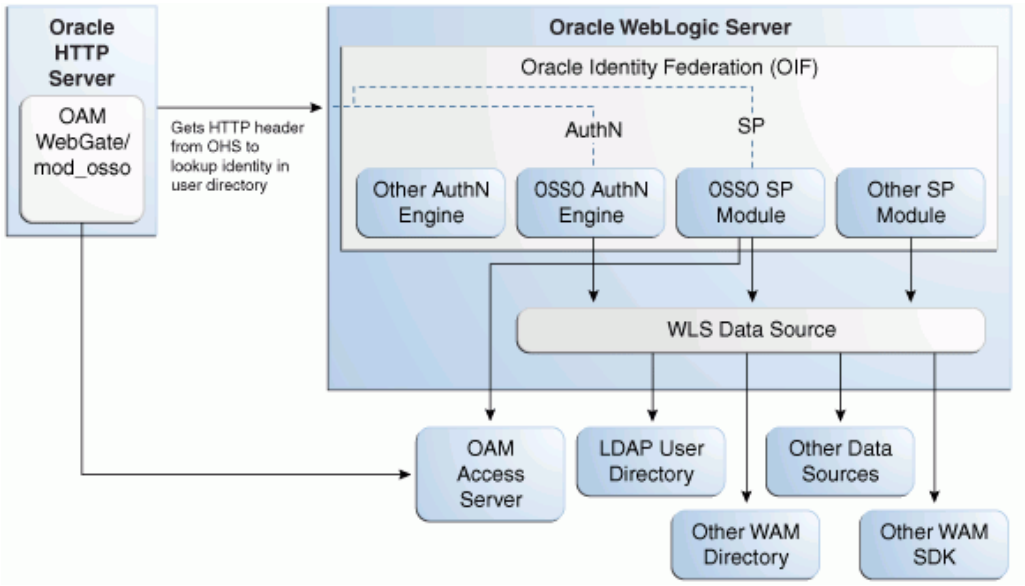
  This mode enables Oracle Identity Federation to authenticate the user via Federation SSO and propagate the authentication state to Access Manager, which maintains the session information.

- Authentication Mode

  This mode enables Access Manager to authenticate the user on behalf of Oracle Identity Federation.

Figure 6-1 describes the processing flow in each mode:

Figure 6-1 Access Manager with Identity Federation



In the SP mode, Oracle Identity Federation uses the federation protocols to identify a user, and requests Access Manager to create an authenticated session at Access Manager.

In the authentication mode, Oracle Identity Federation delegates authentication to Access Manager through the use of a WebGate agent protecting an Oracle Identity Federation resource. Once the user is authenticated, the WebGate will assert the user's identity by an HTTP Header that Oracle Identity Federation will read to identify the user.

6.2.2 Access Manager and Oracle Identity Federation Integration Overview

The integration between Access Manager and Oracle Identity Federation requires the following tasks:

- Ensure that the necessary components, including Oracle WebLogic Server and Identity Management (IdM) components, are installed and operational. For details, see Verifying Servers are Running and a Resource is Protected.
- Register Oracle HTTP Server as a partner with Access Manager to protect a resource. For details, see Registering Oracle HTTP Server WebGate with Access Manager for Access Manager and OIF Integration.
- Configure the Oracle Identity Federation server to function as a service provider (SP) and/or as an identity provider (IdP) with Access Manager. For details, see Configuring Oracle Identity Federation for Access Manager and OIF Integration.
- Configure Access Manager to delegate authentication to Oracle Identity Federation and/or to authenticate a user on behalf of Oracle Identity Federation, For details, see Configuring Access Manager for Integration with Oracle Identity Federation.

6.2.3 Prerequisites to Integrating Access Manager with Oracle Identity Federation

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

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

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

> **See Also:**
>
> About the Oracle Identity and Access Management Installation in *Installing and Configuring Oracle Identity and Access Management*.

6.2.4 Verifying Servers are Running and a Resource is Protected

Check the following components before starting the configuration process:

- 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.

6.2.5 Registering Oracle HTTP Server WebGate with Access Manager for Access Manager and OIF Integration

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

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

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

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

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

2. Make the necessary changes to the file.
3. Locate the `oamreg.sh` script, which resides in the directory:

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

4. Execute the script using the command string:

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

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

   or

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

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

   ```
   http(s)://oif-host:oif-port/fed/user/authnoam11g
   ```

6. Protect this resource with an authentication policy and an authorization policy.
7. Restart Oracle HTTP Server:

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

   You can also restart Oracle HTTP Server with:

   ```
   Oracle_WT1/instances/instance1/bin/opmnctl stopall
   Oracle_WT1/instances/instance1/bin/opmnctl startall
   ```

6.2.6 Configuring Oracle Identity Federation for Access Manager and OIF Integration

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

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

This section contains these topics:

- Verifying the Oracle Identity Federation User Data Store
- Configuring the Oracle Identity Federation Authentication Engine
- Configuring the Oracle Identity Federation SP Integration Module

6.2.6.1 Verifying the Oracle Identity Federation User Data Store

Oracle Identity Federation and Access Manager must use the same LDAP directory:

- The LDAP directory to be used must be defined in Access Manager as the default Identity Store.
- The Oracle Identity Federation User Data Store must reference the LDAP directory to be used.

Take these steps to verify the data store configuration:

1. Locate the Oracle Identity Federation instance in Fusion Middleware Control.
2. Navigate to **Administration**, then **Data Stores**.
3. Ensure that the user data store points to the same directory as the default Access Manager identity store.

6.2.6.2 Configuring the Oracle Identity Federation Authentication Engine

> **Note:**
>
> Running Access Manager-OIF Integration Scripts to Automate Tasks describes scripts that you can execute to automatically perform the manual operations shown here.

Take these steps to configure the Oracle Identity Federation Authentication Engine to retrieve information provided by the WebGate 11g agent:

1. Locate the Oracle Identity Federation instance in Fusion Middleware Control.
2. Navigate to **Administration**, then **Authentication Engines**.
3. Enable the Access Manager 11g authentication engine.
4. Select WebGate 11g as the Agent Type.
5. Enter `OAM_REMOTE_USER` as the User Unique ID Header.
6. In the Default Authentication Engine drop-down list, select Oracle Access Manager 11g.
7. Configure logout:

- If Oracle Identity Federation is also going to be integrated with Access Manager in SP mode, then disable logout as the logout integration with Access Manager 11g will be performed with the OAM11g SP engine.
- If Oracle Identity Federation is not going to be integrated with Access Manager in SP mode:
  - Enable logout
  - Enter the following as the URL:

    ```
    http(s)://oam_host:oam_port/oam/server/logout
    ```

8. Click **Apply**.

6.2.6.3 Configuring the Oracle Identity Federation SP Integration Module

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

> **Note:**
>
> Running Access Manager-OIF Integration Scripts to Automate Tasks describes scripts that you can execute to automatically perform the manual operations shown here.

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 Access Manager 11g tab.
4. Configure the page as follows:
   - Check the **Enable SP Module** box.
   - In the Default SP Integration Module drop-down, select Oracle Access Manager 11g.
   - Check the **Logout Enabled** box.
   - Configure these URLs:

     ```
     Login URL :  http(s)://oam_host:oam_port/oam/server/dap/cred_submit
     Logout URL:  http(s)://oam_host:oam_port/oam/server/logout
     ```

     where *oam_host* and *oam_port* are the host and port number of the Access Manager server respectively.
   - Set Username Attribute value to "cn" to match the Access Manager username attribute.
   - Click **Apply**.
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 Access Manager and Oracle

Identity Federation servers. Be sure to save the keystore file using the **Save As** dialog.

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

> **Note:**
>
> Make a note of the location, since you will need to refer to it later.

6.2.7 Configuring Access Manager for Integration with Oracle Identity Federation

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

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

This section contains these topics:

- Configuring Access Manager to Redirect Users to Oracle Identity Federation
- Registering Oracle Identity Federation as a Trusted Access Manager Partner

6.2.7.1 Configuring Access Manager to Redirect Users to Oracle Identity Federation

This task configures Access Manager to redirect the user to Oracle Identity Federation for authentication when `OIFScheme` is used to protect a resource using Federation single sign-on. The steps needed to achieve this are as follows:

1. Log in to the Oracle Access Management Console:

   `http://oam_adminserver_host:oam_adminserver_port/oamconsole`
2. Select the Policy Configuration tab.
3. Select and open the `OIFScheme`.
4. In the Challenge URL field, modify the value of `OIF-Host` and `OIF-Port`:

   `http(s)://oif-host:oif-port/fed/user/spoam11`
5. Confirm that the value of the Context Type drop-down is set to "external".
6. Click **Apply** to save the changes.

6.2.7.2 Registering Oracle Identity Federation as a Trusted Access Manager Partner

If Oracle Identity Federation is used in SP mode only, or authentication and SP mode, refer to Registering Oracle Identity Federation for Use in SP Mode.

If Oracle Identity Federation is used in authentication mode only, refer to Registering Oracle Identity Federation for Use in Authentication Mode.

> **Note:**
>
> Running Access Manager-OIF Integration Scripts to Automate Tasks describes scripts that you can execute to automatically perform the manual operations shown here to register Oracle Identity Federation as a trusted partner.

6.2.7.2.1 Registering Oracle Identity Federation for Use in SP Mode

> **Note:**
>
> Prior to performing this procedure, ensure that OAM Admin Server and all Managed Servers are running.

Copy the keystore file to a directory under the middleware home in which the Access Manager server is installed.

Use a WLST command to update the `OIFDAP` partner block in the `oam-config.xml` configuration file. The steps and syntax are as follows:

1. Enter the shell environment by executing:

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

2. Connect to the Access Manager administration server with the following command syntax:

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

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

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

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

   For example:

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

6.2.7.2.2 Registering Oracle Identity Federation for Use in Authentication Mode

Use a WLST command to update the `OIFDAP` partner block in the `oam-config.xml` configuration file. The steps and syntax are as follows:

1. Enter the shell environment by executing:

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

2. Connect to the Access Manager administration server with the following command syntax:

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

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

```
registerOIFDAPPartnerIDPMode(logoutURL=logoutURL)
```

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

For example:

```
registerOIFDAPPartnerIDPMode(logoutURL="http://abcdef0123.in.mycorp.com:1200/fed/
user/authnslooam11g?doneURL=http://abc1234567.in.mycorp.com:6001/oam/pages/
logout.jsp")
```

6.2.8 Configuring Access Manager to Protect a Resource with the OIFScheme

After the integration of Access Manager and Oracle Identity Federation in SP mode, a resource can now be protected with `OIFScheme`, which will trigger a Federation single sign-on operation when an unauthenticated user requests access to a resource protected by that scheme.

In an Application Domain of the Policy Configuration tab, define an Authentication Policy using the `OIFScheme`, and protect a resource with that authentication policy.

6.2.9 Testing the Access Manager and Oracle Identity Federation Integration Configuration

The final configuration task is to test whether the integration is correctly configured. The steps differ between authentication mode and SP mode.

- Testing the SP Mode Configuration
- Testing the Authentication Mode Configuration

6.2.9.1 Testing the SP Mode Configuration

Take these steps to test for correct configuration in SP mode:

1. Establish federated trust between Oracle Identity Federation and a remote Identity Provider (IdP).
2. Set that identity provider as the default SSO identity provider.
3. Try accessing the protected resource.
4. When set up correctly, you should be redirected to the IdP for authentication. Verify that user credentials are required on this page.
5. Enter valid credentials on the login page.

> **Note:**
>
> The user should exist in both the IdP security domain and the Oracle Identity Federation/Access Manager security domain.

6. Check that you are redirected to the protected page.
7. Verify that the following cookies are created:
   - `OAM_ID`
   - `ORA_OSFS_SESSION`
   - `OHS Cookie`

6.2.9.2 Testing the Authentication Mode Configuration

Take these steps to test for correct configuration in authentication mode:

1. Establish federated trust between Oracle Identity Federation and a remote service provider.
2. Initiate federation single sign-on from the service provider.
3. Verify that you are redirected to the Access Manager login page at the IdP. On this page user credentials are requested.
4. Enter the relevant credentials and process the page.
5. Verify that you are redirected to the service provider domain.

6.3 Running Access Manager-OIF Integration Scripts to Automate Tasks

The automated steps make the integration smoother and faster than a purely manual procedure.

This section describes scripts that automate some of the Oracle Identity Federation configuration tasks described in Integrating Access Manager 11gR2 with Identity Federation 11gR1 for Oracle Access Manager integration.

This section contains these topics:

- Performing Prerequisite Steps Before Integration
- Verifying WebLogic and Oracle Identity Federation Servers are Running
- Executing the Automated Procedure for Access Manager-OIF Integration

6.3.1 Performing Prerequisite Steps Before Integration

The prerequisite procedure is performed before you do anything else for integration. Ensure that the following have been done:

1. The following components are installed:
   - Oracle WebLogic Server
   - Oracle HTTP Server
   - Oracle Access Manager 11*g*
   - Oracle Identity Federation 11*g*

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

For guidance on integration prerequisites, see *Installing and Configuring Oracle Internet Directory*.

2. Oracle Identity Federation 11g and OHS are integrated; that is, OHS is configured as the front end to the Oracle Identity Federation server.

   For details, see Deploying Oracle Identity Federation with Oracle HTTP Server in *Administrator's Guide for Oracle Identity Federation*.

3. The SSO agent is already created and integrated with Access Manager 11g.

6.3.2 Verifying WebLogic and Oracle Identity Federation Servers are Running

Verify WebLogic and Oracle Identity Federation Servers are running.

- Oracle WebLogic Server

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

- 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.

6.3.3 Executing the Automated Procedure for Access Manager-OIF Integration

Automating some tasks in the integration of Access Manager with Oracle Identity Federation is achieved by executing python scripts provided in the distribution.

Configuring Oracle Identity Federation for Access Manager and OIF Integration describes the tasks that you can automate with scripts.

- Tasks Performed by Federation Configuration Scripts
- Copying the Access Manager-OIF Integration Scripts to the Access Manager Machine
- Understanding Inputs to the Access Manager-OIF Integration Scripts
- Running the Access Manager-OIF Integration Scripts

6.3.3.1 Tasks Performed by Federation Configuration Scripts

The scripts perform the following tasks/procedures:

- Automation of all Oracle Identity Federation configuration
- Registration of Oracle Identity Federationas DAP partner in Access Manager

- Addition of Oracle Identity Federation URLs as protected resources in the policy domain.

6.3.3.2 Copying the Access Manager-OIF Integration Scripts to the Access Manager Machine

You need to copy certain files to the Access Manager host. The files are as follows:

- `setupOIFOAMConfig.sh`,
- `setupOIFOAMIntegration.py`
- locale specific resource bundle `oifWLSTResourceBundle_`*locale*`.properties`

Create a directory to save these files or copy into an existing directory, in the Access Manager host machine. For example, `/scratch/scripts` (linux) or `c:\temp\scripts` (Windows).

6.3.3.3 Understanding Inputs to the Access Manager-OIF Integration Scripts

The script takes in named parameters as inputs (order of inputs does not matter). The inputs mostly have default values if not passed in.

Table 6-2 shows the inputs needed by the scripts:

Table 6-2 Inputs for the Access Manager-OIF 11gR1 Integration Scripts

Parameter	Description	Default	Required?
oifHost	Hostname of Oracle Identity Federation managed server	None	Yes
oifPort	Port number of Oracle Identity Federation Managed server	7499	No
oifAdminHost	Hostname of Oracle Identity Federation Admin server	oifHost	No
oifAdminPort	Port number of Oracle Identity Federation Admin server	7001	No
oamAdminHost	Hostname of Access Manager Admin server	localhost	No
oamAdminPort	Port number of Access Manager Admin server	7001	No
agentType	Agent type used, such as webgate10g, webgate11g, mod_osso	webgate11g	No

> **Note:**
>
> The agent type is the agent created in Access Manager using the `rreg` tool or through the Oracle Access Management Console.

6.3.3.4 Running the Access Manager-OIF Integration Scripts

The automation is run by executing the script file `setupOIFOAMConfig.sh` (Linux) or `setupOIFOAMConfig.cmd` (Windows).

The steps are as follows:

On Unix:

The following steps show how to run the script. Substitute the sample parameter values with appropriate values.

1. In a command line prompt set the `DOMAIN_HOME`:

   ```
   export DOMAIN_HOME=path to domain home
   ```

2. If Oracle Identity Federation administration and managed server are on the same host and the agent type is non-default (for example, webgate10g), execute the command:

   ```
   ./setupOIFOAMConfig.sh oifHost=myhost oifPort=portnum oamAdminHost=myhost2
   oamAdminPort=portnum2 agentType=webgate10g
   ```

3. If Oracle Identity Federation administration and managed server are on different hosts, with a default agent type (webgate11g), execute the command:

   ```
   ./setupOIFOAMConfig.sh oifHost=myhost oifPort=portnum oifAdminHost=myhost2
   oifAdminPort=portnum2 oamAdminHost=myhost3 oamAdminPort=portnum3
   ```

4. If Oracle Identity Federation administration and managed server are on the same host, and all defaults apply from Table 6-2, execute the command:

   ```
   ./setupOIFOAMConfig.sh oifHost=myhost oamAdminHost=myhost2
   ```

On Windows:

The following steps show how to run the script. Substitute the sample parameter values with appropriate values.

1. In a command line prompt set the `DOMAIN_HOME`:

   ```
   set DOMAIN_HOME=path to oam domain home
   ```

2. If Oracle Identity Federation administration and managed server are on the same host and the agent type is non-default (for example, webgate10g), execute the command:

   ```
   setupOIFOAMConfig.cmd  "oifHost=myhost" "oifPort=portnum" "oamAdminHost=myhost2"
   "oamAdminPort=portnum2" "agentType=webgate10g"
   ```

3. If Oracle Identity Federation administration and managed server are on different hosts, with a default agent type (webgate11g), execute the command:

   ```
   setupOIFOAMConfig.cmd "oifHost=myhost" "oifPort=portnum" "oifAdminHost=myhost2"
   "oifAdminPort=portnum2" "oamAdminHost=myhost3" "oamAdminPort=portnum3"
   ```

4. If Oracle Identity Federation administration and managed server are on the same host, and all defaults apply from Table 6-2, execute the command:

   ```
   setupOIFOAMConfig.cmd "oifHost=myhost" " "oamAdminHost=myhost3"
   ```

Part IV
Additional Identity Store Configuration

This part contains topics related to additional configuration of the identity store.

This part contains the following chapter:

- Configuring an Identity Store with Multiple Directories

7

Configuring an Identity Store with Multiple Directories

This chapter explains how to prepare directories other than Oracle Internet Directory for use as an Identity Store.
This chapter contains the following topics:

7.1 Overview of Configuring Multiple Directories as an Identity Store

This chapter describes how to configure Oracle Virtual Directory for two multiple directory scenarios. In both scenarios, you have some user data in a third-party directory, such as Active Directory, and other user data in Oracle Internet Directory.

In both scenarios, you use Oracle Virtual Directory to present all the identity data in a single consolidated view that Oracle Identity Management components can interpret.

The scenarios are as follows:

- **Split Profile**: A split profile, or split directory configuration, is one where identity data is stored in multiple directories, possibly in different locations. You use a split profile when you must extend directory schema in order to support specific schema elements, but you cannot or do not want to extend the schema in the third-party Identity Store. In that case, deploy an Oracle Internet Directory as a shadow directory to store the extended attributes. For details, see Configuring Multiple Directories as an Identity Store: Distinct User and Group Populations in Multiple Directories . (If, on the other hand, you can extend the schema, use the approach described in Section 2.2.3, "Extending the Directory Schema for Access Manager.")
- **Distinct User and Group Populations**: Another multidirectory scenario is one where you have distinct user and group populations, such as internal and external users. In this configuration, Oracle-specific entries and attributes are stored in Oracle Internet Directory. Enterprise-specific entries, for example, entries with Fusion Applications-specific attributes, are stored in Active Directory. For details, see Configuring Multiple Directories as an Identity Store: Distinct User and Group Populations in Multiple Directories .

In this chapter, Active Directory is chosen as the non-Oracle Internet Directory Enterprise Directory. The solution is applicable to all enterprises having one or more Active Directories as their enterprise Identity Store.

7.2 Configuring Multiple Directories as an Identity Store: Split Profile

This section describes how to configure multiple directories as an Identity Store. In cases where the Active Directory schema cannot be extended, you use Oracle Internet Directory as a shadow directory to store these attributes. Oracle Virtual Directory links them together to present a single consolidated DIT view to clients. This is called a split profile or split directory configuration. In this configuration, all the Oracle specific attributes and Oracle specific entities are created in Oracle Internet Directory.

This section contains the following topics:

7.2.1 Prerequisites to Configuring Multiple Directories as an Identity Store

The following assumptions and rules apply to this deployment topology:

- Oracle Internet Directory houses the Fusion Identity Store. This means that Oracle Internet Directory is the store for all Fusion Application-specific artifacts. The artifacts include a set of enterprise roles used by Fusion Application and some user attributes required by Fusion Applications. All other stores are referred to as enterprise Identity Stores.
- The enterprise contains more than one LDAP directory. Each directory contains a distinct set of users and roles.
- The enterprise policy specifies that specific user attributes, such as Fusion Application-specific attributes, cannot be stored in the enterprise directory. All the extended attributes must be stored in a separate directory called the shadow directory. This shadow directory must be Oracle Internet Directory because Active Directory does not allow you to extend the schema.
- User login IDs are unique across the directories. There is no overlap of the user login IDs between these directories.
- Oracle Identity Management has no fine-grained authorization. If Oracle Identity Management's mapping rules allow it to use one specific subtree of a directory, then it can perform all CRUD (Create, Read, Update, Delete) operations in that subtree of the LDAP directory. There is no way to enable Oracle Identity Management to read user data in a subtree but not enable it to create a user or delete a user in subtree.

- Referential integrity must be turned off in Oracle Internet Directory so that an Oracle Internet Directory group can have members that are in one of the Active Directory directories. The users group memberships are not maintained across the directories with referential integrity.

7.2.2 Repository Descriptions

This section describes the artifacts in the Identity store and how they can be distributed between Active Directory and Oracle Internet Directory, based on different enterprise deployment requirements.

The Artifacts that are stored in the Identity Store are:

- Application IDs: These are the identities that are required to authenticate applications to communicate with each other.
- Seeded Enterprise Roles: These are the enterprise roles or LDAP group entries that are required for default functionality.
- Enterprise roles provisioned by Oracle Identity Management: These are runtime roles.
- Enterprise Users: These are the actual users in the enterprise.
- Enterprise Groups: These are the roles and groups that already exist in the enterprise.

In a split profile deployment, the Identity Store artifacts can be distributed among Active Directory and Oracle Internet Directory, as follows.

- Oracle Internet Directory is a repository for enterprise roles. Specifically, Oracle Internet Directory contains the following:
  - Application IDs
  - Seeded enterprise roles
  - Enterprise roles provisioned by Oracle Identity Management
- Active Directory is the repository for:
  - Enterprise users
  - Enterprise groups (not visible to Oracle Identity Management or Fusion Applications)

The following limitations apply:

- The Active Directory users must be members of Oracle Internet Directory groups.
- The groups in Active Directory are not exposed at all. Oracle applications only manage the Oracle-created enterprise roles. The groups in Active Directory are not visible to either Oracle Identity Management or Fusion Applications.

7.2.3 Setting Up Oracle Internet Directory as a Shadow Directory

In cases where Oracle Internet Directory is used as the shadow directory to store certain attributes, such as all the Fusion Application-specific attributes, use a separate container in Oracle Internet Directory to store the shadow attributes.

- The Shadow Entries container (`cn=shadowentries`) must be in a separate DIT from the parent of the users and groups container `dc=mycompany,dc=com`, as shown in Figure 7-1.
- The same ACL configured for `dc=mycompany,dc=com` within Oracle Internet Directory must be configured for `cn=shadowentries`. To perform this configuration, use the `ldapmodify` command. The syntax is as follows:

```
ldapmodify -D cn=orcladmin -q -p portNum -h hostname -f ldifFile
```

The following is a sample LDIF file to use with `ldapmodify`:

```
dn: cn=shadowentries
changetype: modify
add: orclaci
orclaci: access to entry by
group="cn=RealmAdministrators,cn=groups,cn=OracleContext,dc=mycompany,dc=com"
 (browse,add,delete)
orclaci: access to attr=(*) by
group="cn=RealmAdministrators,cn=groups,cn=OracleContext,dc=mycompany,dc=com"
 (read, write, search, compare)
orclaci: access to entry by
group="cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com"
(browse,add,delete)
orclaci: access to attr = (*) by
group="cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com"
(search,read,compare,write)
-
changetype: modify
add: orclentrylevelaci
orclentrylevelaci: access to entry by * (browse,noadd,nodelete)
orclentrylevelaci: access to attr=(*) by * (read,search,nowrite,nocompare)
```

- If you have more than one directory for which Oracle Internet Directory is used as a Shadow directory, then you must create different shadow containers for each of the directories. The container name can be chosen to uniquely identify the specific directory for which this is a shadow entry.

7.2.4 Directory Structure Overview - Shadow Join

Figure 7-1 shows the directory structure in the primary and shadow directories. The containers `cn=reservation`, `cn=appIDUsers`, `cn=FusionGroups`, and `cn=DataRoleGroups` are speciric to Fusion Applications.

Figure 7-1 Directory Structure

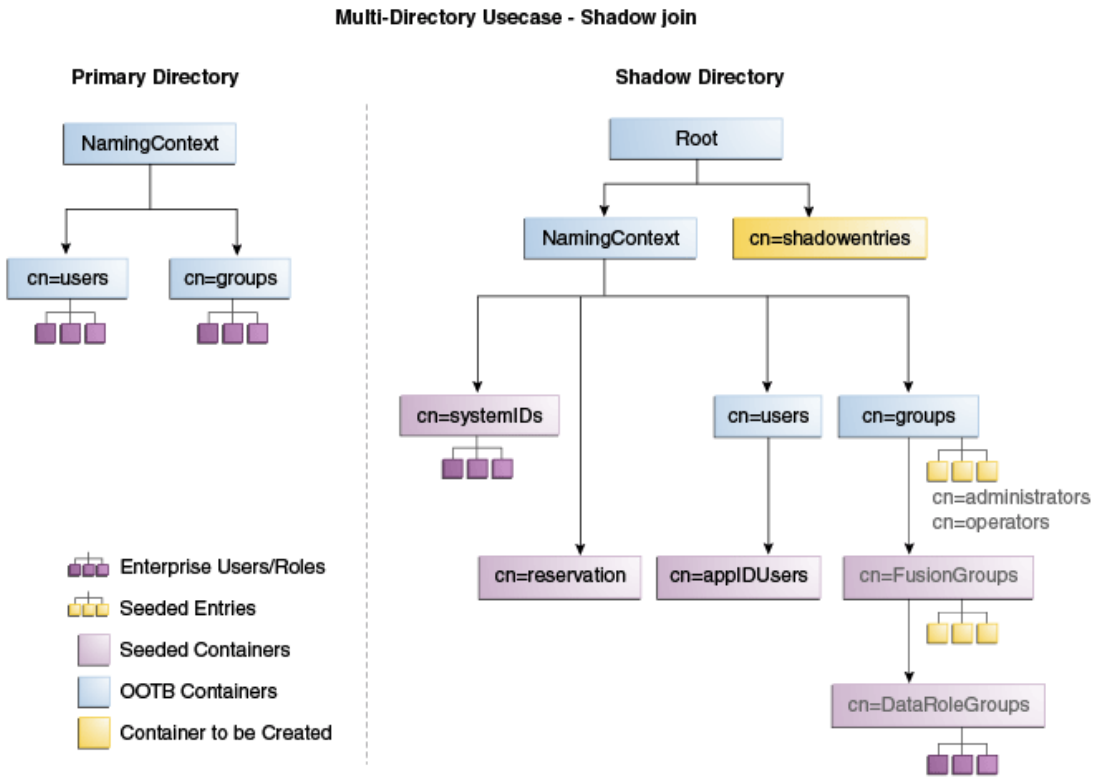


Figure 7-2 shows how the DIT appears to a user or client application. The containers `cn=appIDUsers`, `cn=FusionGroups`, and `cn=DataRoleGroups` are speciric to Fusion Applications.

Figure 7-2 Client View of the DIT

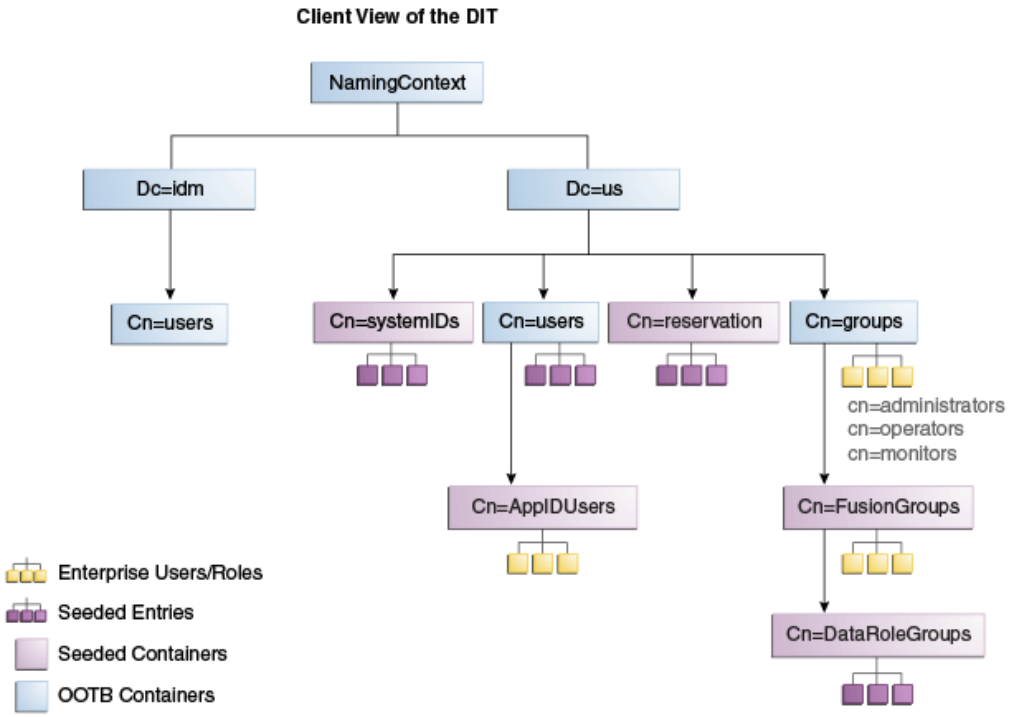
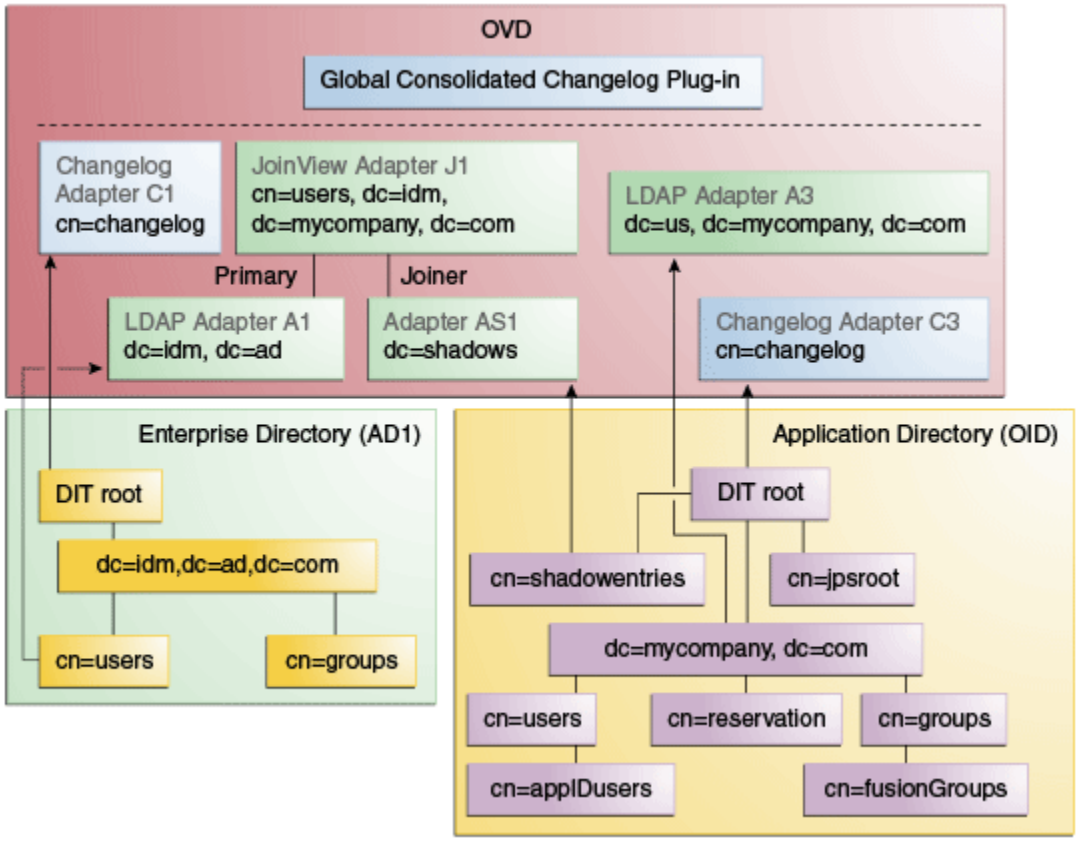


Figure 7-3 summarizes the adapters and plug-ins. The containers `cn=appIDUsers`, and `cn=FusionGroups` are speciric to Fusion Applications.

Figure 7-3 Adapter and Plug-in Configuration



7.2.5 Configuring Oracle Virtual Directory Adapters for Split Profile

In order to produce the client side view of the data shown in Figure 7-2, you must configure multiple adapters in Oracle Virtual Directory following the steps in this section.

You can use `idmConfigTool` to create the adapters to facilitate this configuration.

> **See Also:**
>
> Section A.1, "Verifying Oracle Virtual Directory Adapters for Split Profile by Using ODSM" for instructions on viewing the adapters using Oracle Directory Services Manager.

To create the adapters using `idmConfigTool`, perform the following tasks on IDMHOST1:

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

   Set *`IDM_HOME`* to *`IDM_ORACLE_HOME`*

   Set *`ORACLE_HOME`* to *`IAM_ORACLE_HOME`*

2. Create a properties file for the adapter you are configuring called `splitprofile.props`, with the following content:

```
ovd.host:ldaphost1.mycompany.com
ovd.port:8899
ovd.binddn:cn=orcladmin
ovd.ssl:true
ldap1.type:AD
ldap1.host:adhost.mycompany.com
ldap1.port:636
ldap1.binddn:administrator@idmqa.com
ldap1.ssl:true
ldap1.base:dc=idmqa,dc=com
ldap1.ovd.base:dc=idmqa,dc=com
usecase.type:split
ldap2.type:OID
ldap2.host:ldaphost.mycompany.com
ldap2.port:3060
ldap2.binddn:cn=oimLDAP,cn=users,dc=mycompany,dc=com
ldap2.ssl:false
ldap2.base:dc=mycompany,dc=com
ldap2.ovd.base:dc=mycompany,dc=com
```

The following list describes the parameters used in the properties file.

- `ovd.host` is the host name of a server running Oracle Virtual Directory.
- `ovd.port` is the https port used to access Oracle Virtual Directory.
- `ovd.binddn` is the user DN you use to connect to Oracle Virtual Directory.
- `ovd.password` is the password for the DN you use to connect to Oracle Virtual Directory.
- `ovd.oamenabled` is set to `true` if you are using Oracle Access Management Access Manager, otherwise set to `false`.

  `ovd.oamenabled` is always `true` in Fusion Applications deployments.
- `ovd.ssl` is set to `true`, as you are using an https port.
- `ldap1.type` is set to OID for the Oracle Internet Directory back end directory or set to AD for the Active Directory back end directory.
- `ldap1.host` is the Active Directory host. Use the load balancer name where the host is highly available.
- `ldap2.host`: The Oracle Internet Directory host. Use the load balancer name where the host is highly available.
- `ldap1.port` is the port used to communicate with the back end directory.
- `ldap1.binddn` is the bind DN of the `oimLDAP` user.
- `ldap1.password` is the password of the `oimLDAP` user
- `ldap1.ssl` is set to `true` if you are using the back end's SSL connection, and otherwise set to `false`. This should always be set to `true` when an adapter is being created for AD.
- `ldap1.base` is the base location in the directory tree.
- `ldap1.ovd.base` is the mapped location in Oracle Virtual Directory.

- `usecase.type` is set to `Single` when using a single directory type.

3. Configure the adapter by using the `idmConfigTool` command, which is located at:

   IAM_ORACLE_HOME/idmtools/bin

> **Note:**
>
> When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:
>
> *IAM_ORACLE_HOME*/idmtools/bin

The syntax of the command on Linux is:

```
idmConfigTool -configOVD input_file=splitprofile.props
```

During the running of the command you will be prompted for the passwords to each of the directories you will be accessing.

The command must be run once for each Oracle Virtual Directory instance.

7.2.6 Configuring a Global Consolidated Changelog Plug-in

Deploy a global level consolidated changelog plug-in to handle changelog entries from all the Changelog Adapters.

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to an Oracle Virtual Directory instance.
3. On the Home page, click the **Advanced** tab. The Advanced navigation tree appears.
4. Expand **Global Plugins**
5. Click the **Create Plug-In** button. The Plug-In dialog box appears.
6. Enter a name for the Plug-in in the Name field.
7. Select the plug-in class **ConsolidatedChglogPlugin** from the list.
8. Click **OK**.
9. Click **Apply**.

7.2.7 Validating the Oracle Virtual Directory Changelog

Run the following command to validate that the changelog adapter is working:

```
$IDM_ORACLE_HOME/bin/ldapsearch -p 6501 -D cn=orcladmin -q -b 'cn=changelog' -s base
'objectclass=*' lastchangenumber
```

The command should return a changelog result, such as:

```
Please enter bind password:
cn=Changelog
lastChangeNumber=changelog_OID:190048;changelog_AD1:363878
```

If `ldapsearch` does not return a changelog result, double check the changelog adapter configuration.

7.3 Configuring Multiple Directories as an Identity Store: Distinct User and Group Populations in Multiple Directories

In this configuration, you store Oracle-specific entries in Oracle Internet Directory and enterprise-specific entries in Active Directory. If necessary, extend the Active Directory schema. See Configuring Active Directory for Use with Oracle Access Manager and Oracle Identity Governance in *Oracle® Fusion Middleware Enterprise Deployment Guide for Oracle Identity and Access Management*.

> **Note:**
>
> The Oracle Internet Directory that is to be used is not necessarily the PolicyStore Oracle Internet Directory. Conceptually, a non-Active Directory directory can be used as the second directory. For convenience, this section refers to the Policy Store Oracle Internet Directory.

The following conditions are assumed:

- Enterprise Directory Identity data is in one or more directories. Application-specific attributes of users and groups are stored in the Enterprise Directory.
- Application-specific entries are in the Application Directory. AppIDs and Enterprise Roles are stored in the Application Directory,

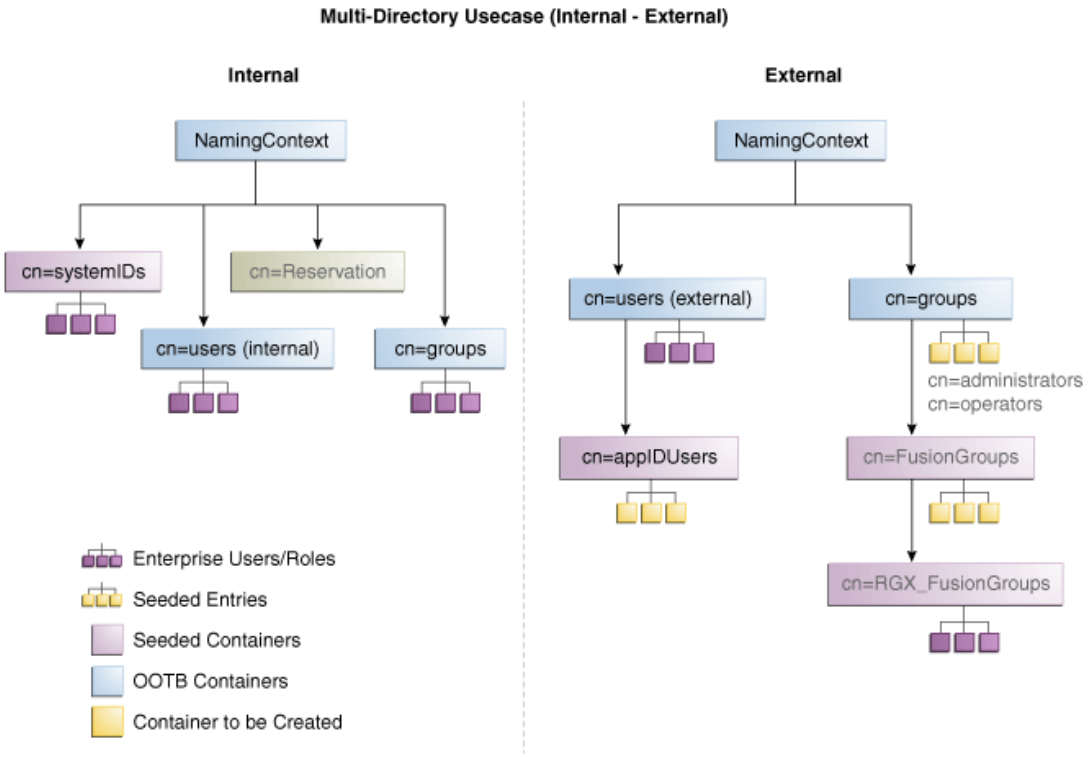
This section contains the following topics:

- Directory Structure Overview for Distinct User and Group Populations in Multiple Directories
- Configuring Oracle Virtual Directory Adapters for Distinct User and Group Populations in Multiple Directories
- Creating a Global Plug-in

7.3.1 Directory Structure Overview for Distinct User and Group Populations in Multiple Directories

Figure 7-4 shows the directory structure in the two directories, listed here as internal and external. The containers cn=appIDUsers, cn=FusionGroups, and cn=RGX_FusionGroups are Fusion Applications-specific.

Figure 7-4 Directory Structure



Oracle Virtual Directory makes multiple directories look like a single DIT to a user or client application, as shown in Figure 7-5. The containers cn=appIDUsers, cn=FusionGroups, and cn=RGX_FusionGroups are Fusion Applications-specific.

Figure 7-5 Client View of the DIT

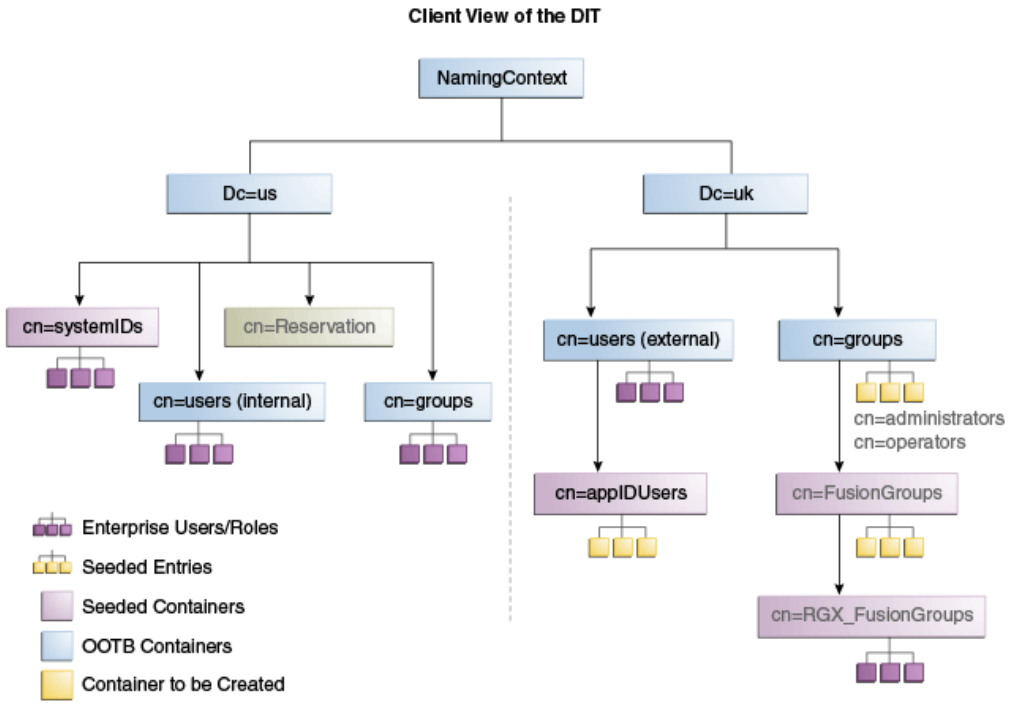
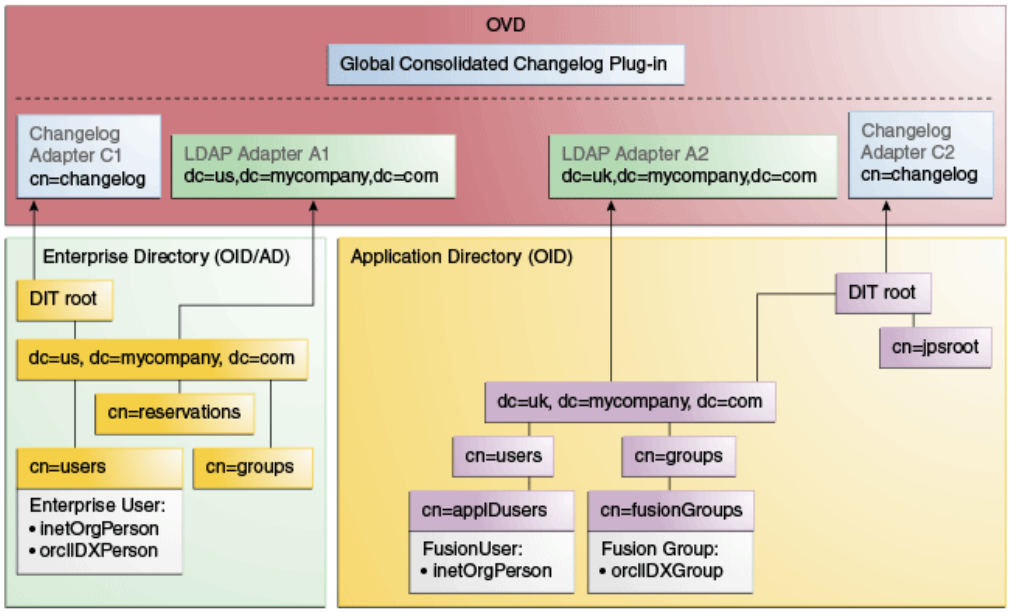


Figure 7-6 provides an overview of the adapter configuration. The classes `inetOrgPerson`, `orclIDXPerson`, and `orclIDXGroup` and the containers `cn=appIDusers` and `cn=fusionGroups` are required only for Fusion Applications.

Figure 7-6 Configuration Overview



7.3.2 Configuring Oracle Virtual Directory Adapters for Distinct User and Group Populations in Multiple Directories

Create the user adapter on the Oracle Virtual Directory instances running on LDAPHOST1 and LDAPHOST2 individually, as described in the following sections:

- Creating Enterprise Directory Adapters
- Creating Application Directory Adapters

7.3.2.1 Creating Enterprise Directory Adapters

Create Oracle Virtual Directory adapters for the Enterprise Directory. The type of adapter that is created will be dependent on whether or not the back end directory resides in Oracle Internet Directory or Active Directory.

You can use `idmconfgTool` to create the Oracle Virtual Directory User and Changelog adapters for Oracle Internet Directory and Active Directory.

> **See Also:**
>
> Section A.1 for instructions on viewing the adapters using Oracle Directory Services Manager.

Oracle Identity Management requires adapters. It is highly recommended, though not mandatory, that you use Oracle Virtual Directory to connect to Oracle Internet Directory.

To create the adapters using `idmconfgTool`, perform the following tasks on IDMHOST1:

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

   Set *`IDM_HOME`* to *`IDM_ORACLE_HOME`*

   Set *`ORACLE_HOME`* to *`IAM_ORACLE_HOME`*

2. Create a properties file for the OID or AD adapter you are configuring called `ovd1.props`, as follows:

   > **Note:**
   >
   > The `usecase.type:single` parameter is not supported for Active Directory through the `configOVD` option.

   Oracle Internet Directory adapter properties file:

```
ovd.host:ldaphost1.mycompany.com
ovd.port:8899
ovd.binddn:cn=orcladmin
ovd.password:ovdpassword
ovd.oamenabled:true
ovd.ssl:true
```

```
ldap1.type:OID
ldap1.host:oididstore.mycompany.com
ldap1.port:3060
ldap1.binddn:cn=oimLDAP,cn=systemids,dc=mycompany,dc=com
ldap1.ssl:false
ldap1.base:dc=mycompany,dc=com
ldap1.ovd.base:dc=mycompany,dc=com
usecase.type: single
```

Active Directory adapter properties file:

```
ovd.host:ldaphost1.mycompany.com
ovd.port:8899
ovd.binddn:cn=orcladmin
ovd.password:ovdpassword
ovd.oamenabled:true
ovd.ssl:true
ldap1.type:AD
ldap1.host:adidstore.mycompany.com
ldap1.port:636
ldap1.binddn:cn=adminuser
ldap1.ssl:true
ldap1.base:dc=mycompany,dc=com
ldap1.ovd.base:dc=mycompany,dc=com
usecase.type: single
```

The following list contains the parameters used in the properties file and their descriptions.

- `ovd.host` is the host name of a server running Oracle Virtual Directory.
- `ovd.port` is the https port used to access Oracle Virtual Directory.
- `ovd.binddn` is the user DN you use to connect to Oracle Virtual Directory.
- `ovd.password` is the password for the DN you use to connect to Oracle Virtual Directory.
- `ovd.oamenabled` is set to `true` if you are using Oracle Access Management Access Manager, otherwise set to `false`.

  `ovd.oamenabled` is always `true` in Fusion Applications deployments.
- `ovd.ssl` is set to `true`, as you are using an https port.
- `ldap1.type` is set to OID for the Oracle Internet Directory back end directory or set to AD for the Active Directory back end directory.
- `ldap1.host` Back end directory host.
- `ldap1.port` is the port used to communicate with the back end directory.
- `ldap1.binddn` is the bind DN of the `oimLDAP` user.
- `ldap1.password` is the password of the `oimLDAP` user
- `ldap1.ssl` is set to `true` if you are using the back end's SSL connection, and otherwise set to `false`. This should always be set to `true` when an adapter is being created for AD.
- `ldap1.base` is the base location in the directory tree.
- `ldap1.ovd.base` is the mapped location in Oracle Virtual Directory.
- `usecase.type` is set to `Single` when using a single directory type.

3. Configure the adapter by using the `idmConfigTool` command, which is located at:

   IAM_ORACLE_HOME/idmtools/bin

   > **Note:**
   >
   > When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:
   >
   > *IAM_ORACLE_HOME*/idmtools/bin

   The syntax of the command on Linux is:

   ```
   idmConfigTool.sh -configOVD input_file=configfile [log_file=logfile]
   ```

   The syntax on Windows is:

   ```
   idmConfigTool.bat -configOVD input_file=configfile [log_file=logfile]
   ```

   For example:

   ```
   idmConfigTool.sh -configOVD input_file=ovd1.props
   ```

   The command requires no input. The output looks like this:

   ```
   The tool has completed its operation. Details have been logged to logfile
   ```

Run this command on each Oracle Virtual Directory host in your topology, with the appropriate value for `ovd.host` in the property file.

7.3.2.2 Creating Application Directory Adapters

Create Oracle Virtual Directory adapters for the Application Directory. The back end directory for the application directory is always Oracle Internet Directory.

You can use `idmconfgTool` to create the Oracle Virtual Directory User and Changelog adapters for Oracle Internet Directory and Active Directory. Oracle Identity Management requires adapters. It is highly recommended, though not mandatory, that you use Oracle Virtual Directory to connect to Oracle Internet Directory.

To do this, perform the following tasks on IDMHOST1:

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

   Set *IDM_HOME* to *IDM_ORACLE_HOME*

   Set *ORACLE_HOME* to *IAM_ORACLE_HOME*

2. Create a properties file for the adapter you are configuring called `ovd1.props`. The contents of this file is as follows.

   Oracle Internet Directory adapter properties file:

   ```
   ovd.host:ldaphost1.mycompany.com
   ovd.port:8899
   ovd.binddn:cn=orcladmin
   ovd.password:ovdpassword
   ```

```
ovd.oamenabled:true
ovd.ssl:true
ldap1.type:OID
ldap1.host:oididstore.mycompany.com
ldap1.port:3060
ldap1.binddn:cn=oimLDAP,cn=systemids,dc=mycompany,dc=com
ldap1.password:oidpassword
ldap1.ssl:false
ldap1.base:dc=mycompany,dc=com
ldap1.ovd.base:dc=mycompany,dc=com
usecase.type: single
```

The following list describes the parameters used in the properties file.

- `ovd.host` is the host name of a server running Oracle Virtual Directory.
- `ovd.port` is the https port used to access Oracle Virtual Directory.
- `ovd.binddn` is the user DN you use to connect to Oracle Virtual Directory.
- `ovd.password` is the password for the DN you use to connect to Oracle Virtual Directory.
- `ovd.oamenabled` is set to `true` if you are using Oracle Access Management Access Manager, otherwise set to `false`.

  `ovd.oamenabled` is always `true` in Fusion Applications deployments.
- `ovd.ssl` is set to `true`, as you are using an https port.
- `ldap1.type` is set to OID for the Oracle Internet Directory back end directory or set to AD for the Active Directory back end directory.
- `ldap1.host` is the host on which back end directory is located. Use the load balancer name.
- `ldap1.port` is the port used to communicate with the back end directory.
- `ldap1.binddn` is the bind DN of the `oimLDAP` user.
- `ldap1.password` is the password of the `oimLDAP` user
- `ldap1.ssl` is set to `true` if you are using the back end's SSL connection, and otherwise set to `false`. This should always be set to `true` when an adapter is being created for AD.
- `ldap1.base` is the base location in the directory tree.
- `ldap1.ovd.base` is the mapped location in Oracle Virtual Directory.
- `usecase.type` is set to `Single` when using a single directory type.

3. Configure the adapter by using the `idmConfigTool` command, which is located at:

   IAM_ORACLE_HOME/idmtools/bin

> **Note:**
>
> When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:
>
> *IAM_ORACLE_HOME*`/idmtools/bin`

The syntax of the command on Linux is:

```
idmConfigTool.sh -configOVD input_file=configfile [log_file=logfile]
```

The syntax on Windows is:

```
idmConfigTool.bat -configOVD input_file=configfile [log_file=logfile]
```

For example:

```
idmConfigTool.sh -configOVD input_file=ovd1.props
```

The command requires no input. The output looks like this:

```
The tool has completed its operation. Details have been logged to logfile
```

Run this command on each Oracle Virtual Directory host in your topology, with the appropriate value for `ovd.host` in the property file.

7.3.3 Creating a Global Plug-in

To create a Global Oracle Virtual Directory plug-in, proceed as follows:

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Create connections to each of the Oracle Virtual Directory instances running on `LDAPHOST1` and `LDAPHOST2`, if they do not already exist.
3. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.
4. On the Home page, click the **Advanced** tab. The Advanced navigation tree appears.
5. Click the + next to **Global Plugins** in the left pane.
6. Click **Create Plugin**.
7. Create the Global Consolidated Changelog Plug-in as follows:

   Enter the following values to create the Global Consolidated Plug-in:

   - **Name**: `Global Consolidated Changelog`
   - **Class**: Click **Select** then choose: **ConsolidatedChangelog**

   Click **OK** when finished.

The environment is now ready to be configured to work with Oracle Virtual Directory as the Identity Store.

7.4 Additional Configuration Tasks When Reintegrating Oracle Identity Governance With Multiple Directories

If you have previously integrated Oracle Identity Management with a single directory and you are now reintegrating it with multiple directories, you must reset the changelog number for each of the incremental jobs to zero. The changelog numbers are repopulated on the next run.

Part V
Appendices

This part contains supplementary content to support the procedures in the book, and includes the following appendices:

- Verifying Adapters for Multiple Directory Identity Stores by Using ODSM
- Using the idm.conf File
- Using the idmConfigTool Command
- Configuring User-Defined Fields
- Modifying OIG to Revert OIG-OAM Integration Configuration
- Upgrading OIG-OAM Integrated Environments

A

Verifying Adapters for Multiple Directory Identity Stores by Using ODSM

After you have configured your Oracle Virtual Directory adapters as described in Chapter 6, "Configuring an Identity Store with Multiple Directories," you can use ODSM to view the adapters for troubleshooting purposes. This chapter explains how.
This appendix contains the following sections:

- Verifying Oracle Virtual Directory Adapters for Split Profile by Using ODSM
- Verifying Adapters for Distinct User and Group Populations in Multiple Directories by Using ODSM

A.1 Verifying Oracle Virtual Directory Adapters for Split Profile by Using ODSM

This section describes how to validate the adapters created in Configuring Oracle Virtual Directory Adapters for Split Profile.

This section contains the following topics:

- Verifying User Adapter for Active Directory Server
- Verifying Shadowjoiner User Adapter
- Verifying JoinView Adapter
- Verifying User/Role Adapter for Oracle Internet Directory
- Verifying Changelog Adapter for Active Directory Server
- Verifying Changelog Adapter for Oracle Internet Directory
- Configuring a Global Consolidated Changelog Plug-in
- Validating Oracle Virtual Directory Changelog

A.1.1 Verifying User Adapter for Active Directory Server

Verify the following adapter and plug-ins for Active Directory:

Follow these steps to verify the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM). The URL is of the form: `http://admin.mycompany.com/odsm`.
2. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.
3. On the Home page, click the **Adapter** tab.
4. Click **user_AD1** adapter.

5. Verify that the User Adapter routing as configured correctly:
   a. **Visibility** must be set to internal.
   b. **Bind Support** must be set to enable.
6. Verify the User Adapter User Management Plug-in as follows:
   a. Select the **User Adapter**.
   b. Click the **Plug-ins** tab.
   c. Click the **User Management** Plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
   d. Verify that the plug-in parameters are as follows:

Parameter	Value	Default
directoryType	`activedirectory`	`Yes`
exclusionMapping	`orclappiduser,uid=samaccountname`	
mapAttribute	`orclguid=objectGuid`	
mapAttribute	`uniquemember=member`	
addAttribute	`user,samaccountname=%uid%,%orclshortuid%`	
mapAttribute	`mail=userPrincipalName`	
mapAttribute	`ntgrouptype=grouptype`	
mapObjectclass	`groupofUniqueNames=group`	
mapObjectclass	`orclidxperson=user`	
pwdMaxFailure	10	`Yes`
oamEnabled	`True`[1]	
mapObjectClass	`inetorgperson=user`	`Yes`
mapPassword	`True`	`Yes`
oimLanguages	Comma separated list of language codes, such as `en,fr,ja`	

[1] Set oamEnabled to true only if you are using Oracle Access Management Access Manager.

A.1.2 Verifying Shadowjoiner User Adapter

Follow these steps to verify the ShadowJoiner Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to Oracle Virtual Directory.
3. On the Home page, click the **Adapter** tab.
4. Click the **Shadow4AD1** Adapter.
5. Ensure that User Adapter routing as is configured correctly:
   a. **Visibility** must be set to internal.

b. **Bind Support** must be set to enable.

6. Verify the User Adapter as follows:
   a. Select the User Adapter.
   b. Click the **Plug-ins** tab.
   c. Click the **User Management** Plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
   d. Verify that the parameters are as follows:

Parameter	Value	Default
directoryType	`oid`	`Yes`
pwdMaxFailure	`10`	`Yes`
oamEnabled	`true`	
mapObjectclass	`container=orclContainer`	`Yes`
oimDateFormat	yyyyMMddHHmmss'z'	

A.1.3 Verifying JoinView Adapter

Follow these steps to verify the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to the Oracle Directory Services Manager (ODSM) page.
2. Connect to Oracle Virtual Directory.
3. On the Home page, click the **Adapter** tab.
4. Click the JoinView adapter.
5. Verify the Adapter as follows
   a. Click **Joined Adapter** in the adapter tree. It should exist
   b. Click **OK**.

A.1.4 Verifying User/Role Adapter for Oracle Internet Directory

Follow these steps to verify the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to Oracle Virtual Directory.
3. On the Home page, click the **Adapter** tab.
4. Click User Adapter.
5. Verify the plug-in as follows:
   a. Select the User Adapter.
   b. Click the **Plug-ins** tab.
   c. Click the **User Management** Plug-in in the plug-ins table, then click **Edit**. The plug-in editing window appears.

d. Verify that the parameters are as follows:

Parameter	Value	Default
directoryType	`oid`	`Yes`
pwdMaxFailure	`10`	`Yes`
oamEnabled	`true`	
mapObjectclass	`container=orclContainer`	`Yes`
oimDateFormat	yyyyMMddHHmmss'z'	

e. Click **OK**.

A.1.5 Verifying Changelog Adapter for Active Directory Server

Follow these steps to verify the Changelog Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to Oracle Virtual Directory.
3. On the Home page, click the **Adapter** tab.
4. Click the changelog_AD1 adapter.
5. Verify the plug-in as follows.
   a. Select the Changelog Adapter.
   b. Click the **Plug-ins** tab.
   c. In the Deployed Plus-ins table, click the **changelog** plug-in, then click "**Edit** in the plug-ins table. The plug-in editing window appears.
   d. Verify that the parameter values are as follows:

Parameter	Value
directoryType	`activedirectory`
mapAttribute	`targetGUID=objectGUID`
requiredAttribute	`samaccountname`
sizeLimit	`1000`
targetDNFilter	`cn=users,dc=idm,dc=ad,dc=com` The users container in Active Directory
mapUserState	`true`
oamEnabled	`true`
virtualDITAdapterName	user_J1;user_AD1

A.1.6 Verifying Changelog Adapter for Oracle Internet Directory

To use the changelog adapter, you must first enable changelog on the connected directory. To test whether the directory is changelog enabled, type:

```
ldapsearch -h directory_host -p ldap_port -D bind_dn -q -b '' -s base 'objectclass=*'
lastchangenumber
```

for example:

```
ldapsearch -h ldaphost1 -p 389 -D "cn=orcladmin" -q -b '' -s base 'objectclass=*'
lastchangenumber
```

If you see `lastchangenumber` with a value, it is enabled. If it is not enabled, enable it as described in the Enabling and Disabling Changelog Generation by Using the Command Line section of *Administering Oracle Internet Directory*.

Follow these steps to verify the Changelog Adapter in Oracle Virtual Directory using Oracle Directory Services Manager.

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to an Oracle Virtual Directory instance.
3. On the Home page, click the **Adapter** tab.
4. Click the Changelog Adapter.
5. Verify the plug-in as follow.
   a. Select the Changelog Adapter.
   b. Click the **Plug-ins** tab.
   c. In the Deployed Plug-ins table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
   d. Verify that the parameter values are as follows:

Parameter	Value
directoryType	`oid`
mapAttribute	`targetGUID=orclguid`
requiredAttribute	`orclGUID`
modifierDNFilter	`cn=orcladmin`
sizeLimit	`1000`
targetDNFilter	`dc=mycompany,dc=com`
targetDNFilter	cn=shadowentries
mapUserState	`true`
oamEnabled	`true`
virtualDITAdapterName	user_J1;shadow4AD1
virtualDITAdapterName	User Adapter (The name of the User adapter's name)

A.1.7 Configuring a Global Consolidated Changelog Plug-in

Verify the global level consolidated changelog plug-in as follows

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to an Oracle Virtual Directory instance.
3. On the Home page, click the **Advanced** tab. The Advanced navigation tree appears.

4. Expand **Global Plugins**
5. Click the **ConsolidatedChglogPlugin**. The plug-in editing window appears.

A.1.8 Validating Oracle Virtual Directory Changelog

Run the following command to validate that the changelog adapter is working:

```
$IDM_ORACLE_HOME/bin/ldapsearch -p 6501 -D cn=orcladmin -q -b 'cn=changelog' -s
base 'objectclass=*' lastchangenumber
```

The command should return a changelog result, such as:

```
Please enter bind password:
cn=Changelog
lastChangeNumber=changelog_OID:190048;changelog_AD1:363878
```

If `ldapsearch` does not return a changelog result, double check the changelog adapter configuration.

A.2 Verifying Adapters for Distinct User and Group Populations in Multiple Directories by Using ODSM

This section describes how to view the adapters created in Configuring Oracle Virtual Directory Adapters for Distinct User and Group Populations in Multiple Directories.

This section contains the following topics:

- Verifying the User Adapter on the Oracle Virtual Directory Instances
- Verifying the Plug-In of the User/Role Adapter A1
- Verifying the Plug-In of the User/Role Adapter A2
- Verifying the Changelog Adapter C1 Plug-In
- Verifying the Changelog Adapter for Active Directory
- Verifying Changelog Adapter C2
- Verifying Oracle Virtual Directory Global Plug-in
- Configuring a Global Consolidated Changelog Plug-in

A.2.1 Verifying the User Adapter on the Oracle Virtual Directory Instances

Verify the user adapter on the Oracle Virtual Directory instances running on LDAPHOST1 and LDAPHOST2 individually. Follow these steps to verify the User Adapter in Oracle Virtual Directory using Oracle Directory Services Manager:

1. If they are not already running, start the Administration Server and the WLS_ODSM Managed Servers.
2. In a web browser, go to Oracle Directory Services Manager (ODSM) at:

   `http://admin.mycompany.com/odsm`

3. Verify connections to each of the Oracle Virtual Directory instances running on LDAPHOST1 and LDAPHOST2, if they do not already exist.
4. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.
5. On the Home page, click the **Adapter** tab.
6. Click the name of each adapter. Verify that it has the parameters shown in the following tables.

A.2.2 Verifying the Plug-In of the User/Role Adapter A1

Verify the plug-in of the User/Role Adapter A1, as follows:

1. Select the OIM User Adapter.
2. Click the **Plug-ins** tab.
3. Click the **User Management** Plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
4. Verify that the parameter values are as follows:

Parameter	Value	Default
directoryType	`activedirectory`	`Yes`
exclusionMapping	`orclappiduser,uid=samaccountname`	
mapAttribute	`orclguid=objectGuid`	
mapAttribute	`uniquemember=member`	
addAttribute	`user,samaccountname=%uid%,%orclshortuid%`	
mapAttribute	`mail=userPrincipalName`	
mapAttribute	`ntgrouptype=grouptype`	
mapObjectclass	`groupofUniqueNames=group`	
mapObjectclass	`orclidxperson=user`	
pwdMaxFailure	10	`Yes`
oamEnabled	`True`[1]	
mapObjectClass	`inetorgperson=user`	`Yes`
mapPassword	`True`	`Yes`
oimLanguages	Comma separated list of language codes, such as `en,fr,ja`	

[1] Set oamEnabled to true only if you are using Oracle Access Management Access Manager.

A.2.3 Verifying the Plug-In of the User/Role Adapter A2

Verify the plug-in of the User/Role Adapter A2 as follows:

1. Select the User Adapter.
2. Click the **Plug-ins** tab.

3. Click the **User Management** Plug-in in the plug-ins table, then click **Edit**. The plug-in editing window appears.
4. Verify that the parameter values are as follows:

Parameter	Value	Default
directoryType	`oid`	`Yes`
pwdMaxFailure	`10`	`Yes`
oamEnabled	`true`[1]	
mapObjectclass	`container=orclContainer`	`Yes`

[1] Set oamEnabled to true only if you are using Oracle Access Management Access Manager.

A.2.4 Verifying the Changelog Adapter C1 Plug-In

To verify the Changelog Adapter C1 plug-in, follow these steps:

1. Select the OIM changelog adapter **Changelog_Adapter_C1**.
2. Click the **Plug-ins** tab.
3. In the **Deployed Plus-ins** table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
4. In the **Parameters** table, verify that the values are as shown.

Table A-1 Values in Parameters Table

Parameter	Value	Comments
modifierDNFilter	A bind DN that has administrative rights on the directory server, in the format: "!(modifiersname=cn=*BindDN*)" For example: "!(modifiersname=cn=orcladmin,cn=systemids,dc=mycompany,dc=com)"	Create
sizeLimit	1000	Create
targetDNFilter	`dc=us,dc=mycompany,dc=com`	Create
mapUserState	true	Update
oamEnabled	true	Update
virtualDITAdapterName	The adapter name of User/Role Adapter A1: `User_Adapter_A1`	Create

A.2.5 Verifying the Changelog Adapter for Active Directory

Verify the plug-in as follows.

1. Select the OIM Changelog Adapter.
2. Click the **Plug-ins** tab.

3. In the Deployed Plus-ins table, click the **changelog** plug-in, then click "**Edit** in the plug-ins table. The plug-in editing window appears.
4. In the Parameters table, verify that the parameters are as follows:

Parameter	Value
directoryType	`activedirectory`
mapAttribute	`targetGUID=objectGUID`
requiredAttribute	`samaccountname`
sizeLimit	`1000`
targetDNFilter	`dc=mycompany,dc=com` Search base from which reconciliation must happen. This value must be the same as the LDAP SearchDN that is specified during Oracle Identity Governance installation.
mapUserState	`true`
oamEnabled	`true`[1]
virtualDITAdapterName	The name of the User adapter's name

[1] Set oamEnabled to true only if you are using Oracle Access Management Access Manager.

> **Note:**
>
> **virtualDITAdapterName** identifies the corresponding user profile adapter name. For example, in a single-directory deployment, you can set this parameter value to `User Adapter`, which is the user adapter name. In a split-user profile scenario, you can set this parameter to `J1;A2`, where `J1` is the JoinView adapter name, and `A2` is the corresponding user adapter in the `J1`.

A.2.6 Verifying Changelog Adapter C2

Verify the plug-in as follows:

1. Select the OIM changelog adapter **Changelog_Adapter_C2**.
2. Click the **Plug-ins** tab.
3. In the **Deployed Plus-ins** table, click the **changelog** plug-in, then click **Edit** in the plug-ins table. The plug-in editing window appears.
4. In the **Parameters** table, verify that the parameters are as follows:

Table A-2 Values in Parameters Table

Parameter	Value	Comments
modifierDNFilter	A bind DN that has administrative rights on the directory server, in the format: "!(modifiersname=cn=*BindDN*)" For example: "!(modifiersname=cn=orcladmin,dc=mycompany,dc=com)"	Create
sizeLimit	1000	Create
targetDNFilter	dc=uk,dc=mycompany,dc=com	Create
mapUserState	true	Update
oamEnabled	true	Update
virtualDITAdapterName	The adapter name of User/Role adapter A2: User_Adapter_A2	Create

A.2.7 Verifying Oracle Virtual Directory Global Plug-in

To verify the Global Oracle Virtual Directory plug-in, proceed as follows

1. In a web browser, go to Oracle Directory Services Manager (ODSM) at:

   `http://admin.mycompany.com/odsm`

2. Verify connections to each of the Oracle Virtual Directory instances running on LDAPHOST1 and LDAPHOST2, if they do not already exist.
3. Connect to each Oracle Virtual Directory instance by using the appropriate connection entry.
4. On the Home page, click the **Adapter** tab.
5. Click the **Plug-ins** tab.
6. Verify that the Global Consolidated Changelog Plug-in exists.

   Click **OK** when finished.

A.2.8 Configuring a Global Consolidated Changelog Plug-in

Verify the global level consolidated changelog plug-in as follows

1. In a web browser, go to Oracle Directory Services Manager (ODSM).
2. Connect to an Oracle Virtual Directory instance.
3. On the Home page, click the **Advanced** tab. The Advanced navigation tree appears.
4. Expand **Global Plugins**
5. Click the **ConsolidatedChglogPlugin**. The plug-in editing window appears.

B
Using the idm.conf File

This appendix explains the purpose and usage of the idm.conf file for applications with a web interface.
This appendix contains the following topics:

- About the idm.conf File
- Example idm.conf File

B.1 About the idm.conf File

In the Oracle Fusion Middleware environment, the highest level configuration file at the web tier is httpd.conf. This file configures OHS, which processes the web transactions that use the http protocol. OHS processes each incoming request and determines its routing based on the URL from which the request originates and the resource to be accessed.

Additional configuration files are specified in the httpd.conf file by means of the Apache HTTP Server's `Include` directive in an `Ifmodule` block.

Identity management applications in particular make use of the `idm.conf` configuration file, which is a template that administrators can modify to indicate how incoming requests for protected applications must be handled.

The `idm.conf` configuration file is divided into four parts, each addressing a distinct security area or zone. Table B-1 lists the zones:

Table B-1 Zones in the idm.conf File

Zone	Type	Description
1	Default Access Zone	This zone is the default OHS endpoint for all inbound traffic. The protocol is `http` and the context root is in the format `authohs.example.com:7777`.
2	External Access Zone	This zone is the load-balancer (LBR) external end user endpoint. The protocol is `https` and the context root is in the format `sso.example.com:443`.
3	Internal Services Zone	This zone is the LBR internal endpoint for applications. The protocol is `http` and the context root is in the format `idminternal.example.com:7777`.
4	Administrative Services Zone	This zone is the LBR internal endpoint for administrative services. The protocol is `https` and the context root is in the format `admin.example.com:443`.

When updating the `idm.conf` file, be sure to edit only the zone definition applicable to your requirements.

B.2 Example idm.conf File

The following sample shows the layout and different zones of the idm.conf file:

```
NameVirtualHost *:7777

## Default Access
## AUTHOHS.EXAMPLE.COM

<VirtualHost *:7777>
#  ServerName http://authohs.example.com:7777 (replace the ServerName below with
the actual host:port)
   ServerName http://authohs.us.example.com:7777
   RewriteEngine On
   RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end_url=/
console" [R]
   RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em"
[R]
   RewriteRule ^/FSMIdentity/faces/pages/Self.jspx "/oim" [R]
   RewriteRule ^/FSMIdentity/faces/pages/pwdmgmt.jspx "/admin/faces/pages/
pwdmgmt.jspx" [R]
   RewriteOptions inherit
   UseCanonicalName On

# Admin Server and EM

   <Location /console>
      SetHandler weblogic-handler
      WebLogicHost us.example.com
      WeblogicPort 17001
   </Location>

   <Location /consolehelp>
      SetHandler weblogic-handler
      WebLogicHost us.example.com
      WeblogicPort 17001
   </Location>

   <Location /em>
      SetHandler weblogic-handler
      WebLogicHost us.example.com
      WeblogicPort 17001
   </Location>

# FA service

   <Location /fusion_apps>
      SetHandler weblogic-handler
      WebLogicHost us.example.com
      WebLogicPort 14100
   </Location>

#ODSM Related entries
   <Location /odsm>
        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON
        WebLogicHost oidfa.us.example.com
        WeblogicPort 7005
```

```
   </Location>

# OAM Related Entries

   <Location /oamconsole>
      SetHandler weblogic-handler
      WebLogicHost us.example.com
      WebLogicPort 17001
   </Location>

   <Location /oam>
      SetHandler weblogic-handler
      WebLogicHost us.example.com
      WebLogicPort 14100
   </Location>

# OIM Related Entries

# oim identity self service console
<Location /identity>
   SetHandler weblogic-handler
   WLProxySSL ON
   WLProxySSLPassThrough ON
   WLCookieName oimjsessionid
   WebLogicHost us.example.com

    WeblogicPort 14000
 WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>
# oim identity system administration console
  <Location /sysadmin>
     SetHandler weblogic-handler
     WLProxySSL ON
     WLProxySSLPassThrough ON
     WLCookieName oimjsessionid
     WebLogicHost us.example.com
     WeblogicPort 14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>
# oim identity advanced administration console - Legacy 11gR1 webapp
  <Location /oim>
     SetHandler weblogic-handler
     WLProxySSL ON
     WLProxySSLPassThrough ON
     WLCookieName oimjsessionid
     WebLogicHost us.example.com
     WeblogicPort 14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# xlWebApp - Legacy 9.x webapp (struts based)
   <Location /xlWebApp>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# Nexaweb WebApp - used for workflow designer and DM
```

```
   <Location /Nexaweb>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# spml xsd profile
   <Location /spml-xsd>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# used for FA Callback service.
   <Location /callbackResponseService>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# Role-SOD profile
   <Location /role-sod>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# SOA Callback webservice for SOD - Provide the SOA Managed Server Ports
   <Location /sodcheck>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 8001

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# Callback webservice for SOA. SOA calls this when a request is approved/rejected
# Provide the SOA Managed Server Port
   <Location /workflowservice>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# HTTP client service
```

```
   <Location /HTTPClnt>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>


# OIF Related Entries

   <Location /fed>
      SetHandler weblogic-handler
      WebLogicHost us.example.com
      WebLogicPort 7499
   </Location>

</VirtualHost>

## External Access
## SSO.EXAMPLE.COM

<VirtualHost *:7777>
#  ServerName https://sso.example.com:443 (replace the ServerName below with the
actual host:port)
   ServerName https://sso.example.com:443
   RewriteEngine On
   RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end_url=/console"
[R]
   RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em" [R]
   RewriteRule ^/FSMIdentity/faces/pages/Self.jspx "/oim" [R]
   RewriteRule ^/FSMIdentity/faces/pages/pwdmgmt.jspx "/admin/faces/pages/
pwdmgmt.jspx" [R]
   RewriteOptions inherit
   UseCanonicalName On

# FA service
   <Location /fusion_apps>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WebLogicHost us.example.com
      WebLogicPort 14100
   </Location>

# OAM Related Entries

   <Location /oam>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WebLogicHost us.example.com
      WebLogicPort 14100
   </Location>

# OIM Related Entries

# oim identity self service console
<Location /identity>
   SetHandler weblogic-handler
```

```
   WLProxySSL ON
   WLProxySSLPassThrough ON
   WLCookieName oimjsessionid
   WebLogicHost us.example.com

          WeblogicPort 14000
 WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>
# oim identity system administration console
  <Location /sysadmin>
     SetHandler weblogic-handler
     WLProxySSL ON
     WLProxySSLPassThrough ON
     WLCookieName oimjsessionid
     WebLogicHost us.example.com
     WeblogicPort 14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>
# oim identity advanced administration console - Legacy 11gR1 webapp
  <Location /oim>
     SetHandler weblogic-handler
     WLProxySSL ON
     WLProxySSLPassThrough ON
     WLCookieName oimjsessionid
     WebLogicHost us.example.com
     WeblogicPort 14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# xlWebApp - Legacy 9.x webapp (struts based)
   <Location /xlWebApp>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# Nexaweb WebApp - used for workflow designer and DM
   <Location /Nexaweb>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# spml xsd profile
   <Location /spml-xsd>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000
```

```
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# used for FA Callback service.
   <Location /callbackResponseService>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# OIF Related Entries
   <Location /fed>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WebLogicHost weblogic-host.example.com
      WebLogicPort 7499
   </Location>

</VirtualHost>

## IDM Internal services for FA
## IDMINTERNAL.EXAMPLE.COM

<VirtualHost *:7777>
#  ServerName http://idminternal.example.com:7777 (replace the ServerName below with
the actual host:port)
   ServerName http://idminternal.example.com:7777
   RewriteEngine On
   RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end_url=/console"
[R]
   RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em" [R]
   RewriteRule ^/FSMIdentity/faces/pages/Self.jspx "/oim" [R]
   RewriteRule ^/FSMIdentity/faces/pages/pwdmgmt.jspx "/admin/faces/pages/
pwdmgmt.jspx" [R]
   RewriteOptions inherit
   UseCanonicalName On

# FA service
   <Location /fusion_apps>
      SetHandler weblogic-handler
      WebLogicHost us.example.com
      WebLogicPort 14100
   </Location>


# OAM Related Entries

   <Location /oam>
      SetHandler weblogic-handler
      WebLogicHost us.example.com
      WebLogicPort 14100
   </Location>

# OIM Related Entries
```

```
# oim identity self service console
<Location /identity>
   SetHandler weblogic-handler
   WLProxySSL ON
   WLProxySSLPassThrough ON
   WLCookieName oimjsessionid
   WebLogicHost us.example.com

          WeblogicPort 14000
 WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>
# oim identity system administration console
  <Location /sysadmin>
     SetHandler weblogic-handler
     WLProxySSL ON
     WLProxySSLPassThrough ON
     WLCookieName oimjsessionid
     WebLogicHost us.example.com
     WeblogicPort 14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>
# oim identity advanced administration console - Legacy 11gR1 webapp
  <Location /oim>
     SetHandler weblogic-handler
     WLProxySSL ON
     WLProxySSLPassThrough ON
     WLCookieName oimjsessionid
     WebLogicHost us.example.com
     WeblogicPort 14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# xlWebApp - Legacy 9.x webapp (struts based)
   <Location /xlWebApp>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# Nexaweb WebApp - used for workflow designer and DM
   <Location /Nexaweb>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# spml xsd profile
   <Location /spml-xsd>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
```

```
   </Location>

# used for FA Callback service.
   <Location /callbackResponseService>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# Role-SOD profile
   <Location /role-sod>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# SOA Callback webservice for SOD - Provide the SOA Managed Server Ports
   <Location /sodcheck>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 8001

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# Callback webservice for SOA. SOA calls this when a request is approved/rejected
# Provide the SOA Managed Server Port
   <Location /workflowservice>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# HTTP client service
   <Location /HTTPClnt>
      SetHandler weblogic-handler
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# OIF Related Entries

   <Location /fed>
      SetHandler weblogic-handler
      WebLogicHost us.example.com
      WebLogicPort 7499
   </Location>
```

```
</VirtualHost>

## IDM Admin services for FA
## ADMIN.EXAMPLE.COM

<VirtualHost *:7777>
#  ServerName https://admin.example.com:443 (replace the ServerName below with
the actual host:port)
   ServerName https://admin.example.com:443
   RewriteEngine On
   RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end_url=/
console" [R]
   RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em"
[R]
   RewriteRule ^/FSMIdentity/faces/pages/Self.jspx "/oim" [R]
   RewriteRule ^/FSMIdentity/faces/pages/pwdmgmt.jspx "/admin/faces/pages/
pwdmgmt.jspx" [R]
   RewriteOptions inherit
   UseCanonicalName On

# Admin Server and EM

   <Location /console>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WebLogicHost us.example.com
      WeblogicPort 17001
   </Location>

   <Location /consolehelp>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WebLogicHost us.example.com
      WeblogicPort 17001
   </Location>

   <Location /em>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WebLogicHost us.example.com
      WeblogicPort 17001
   </Location>

#ODSM Related entries
   <Location /odsm>
        SetHandler weblogic-handler
        WLProxySSL ON
        WLProxySSLPassThrough ON
        WebLogicHost oidfa.us.example.com
        WeblogicPort 7005
   </Location>

# OAM Related Entries

   <Location /oamconsole>
      SetHandler weblogic-handler
      WLProxySSL ON
```

```
      WLProxySSLPassThrough ON
      WebLogicHost us.example.com
      WebLogicPort 17001
   </Location>


# OIM Related Entries

# oim identity self service console
<Location /identity>
   SetHandler weblogic-handler
   WLProxySSL ON
   WLProxySSLPassThrough ON
   WLCookieName oimjsessionid
   WebLogicHost us.example.com

    WeblogicPort 14000
 WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>
# oim identity system administration console
  <Location /sysadmin>
     SetHandler weblogic-handler
     WLProxySSL ON
     WLProxySSLPassThrough ON
     WLCookieName oimjsessionid
     WebLogicHost us.example.com
     WeblogicPort 14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>
# oim identity advanced administration console - Legacy 11gR1 webapp
  <Location /oim>
     SetHandler weblogic-handler
     WLProxySSL ON
     WLProxySSLPassThrough ON
     WLCookieName oimjsessionid
     WebLogicHost us.example.com
     WeblogicPort 14000
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>


# xlWebApp - Legacy 9.x webapp (struts based)
   <Location /xlWebApp>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# Nexaweb WebApp - used for workflow designer and DM
   <Location /Nexaweb>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000
```

```
    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# HTTP client service
   <Location /HTTPClnt>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WLCookieName oimjsessionid
      WebLogicHost us.example.com
      WeblogicPort 14000

    WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
   </Location>

# OIF Related Entries
   <Location /fed>
      SetHandler weblogic-handler
      WLProxySSL ON
      WLProxySSLPassThrough ON
      WebLogicHost weblogic-host.example.com
      WebLogicPort 7499
   </Location>

</VirtualHost>
```

C

Using the idmConfigTool Command

The IdM configuration tool (`idmConfigTool`) performs a number of tasks to assist in installing, configuring, and integrating Oracle identity management (IdM) components. This appendix explains how to use the tool.

> **Note:**
>
> - This appendix does not contain actual integration procedures; rather, it contains `idmConfigTool` command syntax and related details. Use this appendix as a reference whenever you are executing `idmConfigTool` as directed by your integration procedure or task.
> - Ensure that the LDAP server, as well as the admin servers hosting OAM, OIM are up before you run `idmConfigTool`

This appendix contains these sections:

C.1 About idmConfigTool

This section contains these topics:

C.1.1 What is idmConfigTool?

The `idmConfigTool` helps you to perform the following tasks efficiently:

- To validate configuration properties representing the Identity Management components Oracle Internet Directory (OID), Oracle Virtual Directory (OVD), Oracle Unified Directory

(OUD), Oracle Access Management Access Manager (OAM) and Oracle Identity Governance (OIG).

- To pre-configure the Identity Store components (OID, OVD, and OUD) to install the other Identity Management components, including OAM, OIG, and Oracle Access Management Mobile and Social.
- To post-configure the OAM, OIG components and wiring of those components.
- To extract the configuration of the Identity Management components OID, OVD, OUD, OAM, and OIG.

> **See Also:**
>
> idmConfigTool Command Syntax.

C.1.2 Components Supported by idmConfigTool

`idmConfigTool` supports these 11*g* components:

- Oracle Internet Directory
- Oracle Virtual Directory
- Oracle Access Management Access Manager
- Oracle Identity Management
- Oracle Unified Directory (OUD)
- Oracle Access Management Mobile and Social

C.1.3 When to Use idmConfigTool

Use `idmConfigTool` in these situations:

- Prior to installing Oracle Identity Management and Oracle Access Management Access Manager
- After installing Oracle Identity Management and Oracle Access Management Access Manager
- After installing Oracle Access Management Mobile and Social
- When dumping the configuration of IdM components Oracle Internet Directory, Oracle Unified Directory, Oracle Virtual Directory, Oracle Identity Management, and Oracle Access Manager
- When validating the configuration parameters for Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Management, and Oracle Access Manager

What is idmConfigTool? explains the tasks the tool performs in each situation.

C.1.4 Location of idmConfigTool

The `idmConfigTool` is located at:

IAM_ORACLE_HOME`/idmtools/bin`

where *IAM_ORACLE_HOME* is the directory in which OIM and OAM are installed.

To execute idmConfigTool on Linux

```
cd <IAM_ORACLE_HOME>/idmtools/bin
./idmConfigTool.sh
```

To execute idmConfigTool on Windows

```
cd <IAM_ORACLE_HOME>\idmtools\bin
idmConfigTool.cmd
```

C.1.5 Webgate Types Supported by idmConfigTool

The `idmConfigTool` supports OAM 11g Webgates by default. It also supports 10g Webgates.

C.1.6 idmConfigTool in Single- and Cross-Domain Scenarios

The tool supports two types of scenarios with regard to Weblogic domains:

- A single-domain configuration in which both Access Manager and Oracle Identity Management servers are configured in the same Weblogic domain
- A dual or cross-domain configuration in which Access Manager and Oracle Identity Management servers are configured on separate Weblogic domains

C.2 Set Up Environment Variables for OIG-OAM Integration

You must configure the environment before running the `'idmConfigTool`.

Set the following variables:

Table C-1 Environment Variables for `OIGOAMIntegration` script.

Variable	Description
`WL_HOME`	Not mandatory. It is set to `MW_HOME/wlserver_10.3` by default, and this setting is used. See `MW_HOME` for an example.
`JAVA_HOME`	This is the full path of the JDK directory. If running on IBM WebSphere, this variable must point to the IBM JDK. Set the value to the full path of the JDK. For example: `/WASSH/WebSphere/AppServer/java` *Important*: On IBM WebSphere, do not use a JDK other than the IBM JDK.
`ORACLE_HOME`	Set to the full path of the Oracle home. For IdM integrations, set to `IAM_ORACLE_HOME`.

C.3 idmConfigTool Syntax and Usage

This section contains these topics:

- idmConfigTool Command Syntax
- Requirements for Running idmConfigTool

- Files Generated by idmConfigTool
- Using the Properties File for idmConfigTool
- Working with the idmConfigTool Log File

C.3.1 idmConfigTool Command Syntax

The tool has the following syntax on Linux:

```
idmConfigTool.sh -command   input_file=filename log_file=logfileName
log_level=log_level
```

The tool has the following syntax on Windows:

```
idmConfigTool.bat -command   input_file=filename log_file=logfileName
log_level=log_level
```

Values for *command* are as follows:

Command	Component name	Description
`preConfigIDStore`	Identity Store	Configures the identity store and policy store by creating the groups and setting ACIs to the various containers.
`prepareIDStore mode= OAM OIM WLS WAS FUSION OAAM APM all`	Identity Store	Configures the identity store by adding necessary users and associating users with groups. Modes enable you to configure for a specific component. You can run this command on Oracle WebLogic Server (mode=WLS) or IBM WebSphere (mode=WAS).
`configPolicyStore`	Policy Store	Configures policy store by creating read-write user and associates them to the groups.
`configOAM`	Oracle Access Manager Oracle Identity Management	Prepares Access Manager for integration with Oracle Identity Governance.
`configOIM`	Oracle Access Manager Oracle Identity Management	Sets up wiring between Access Manager and Oracle Identity Governance.
`configOMSS`	Oracle Access Management Mobile and Social	Performs post-install configuration for Oracle Access Management Mobile and Social
`configOVD`	Oracle Virtual Directory	Creates OVD adapters.
`disableOVDAccessConfig`	Oracle Virtual Directory	Disables anonymous access to the OVD server. Post-upgrade command. *Note*: `configOVD` performs this task automatically when run.
`postProvConfig`	Identity Store	Performs post-provisioning configuration of the identity store.

Command	Component name	Description
`validate IDSTORE POLICYSTORE OAM11g OAM10g OIM`	Various	Validates the set of input properties for the named entity.
`ovdConfigUpgrade`	Oracle Virtual Directory	Updates the configuration for an upgraded OVD with split profile.
`upgradeLDAPUsersForSSO`	Oracle Identity Management Access Manager	Updates existing users in OID by adding certain object classes which are needed for Oracle Identity Management-Access Manager integration.
`upgradeOIMTo11gWebgate`	Oracle Identity Management Access Manager	Upgrades an existing configuration consisting of integrated Oracle Identity Management-Access Manager, using Webgate 10g, to use Webgate 11g

C.3.2 Requirements for Running idmConfigTool

You must run this tool as a user with administrative privileges when configuring the identity store or the policy store.

The `validate` command requires a component name.

> **Caution:**
>
> The commands cannot be run in isolation. Run them in the context of explicit integration procedures; use this appendix only as a command reference.

C.3.3 Files Generated by idmConfigTool

idmConfigTool creates or updates certain files upon execution.

- Parameter File

  When you run the `idmConfigTool`, the tool creates or appends to the file `idmDomainConfig.param` in the directory from which you run the tool. To ensure that the same file is appended to each time the tool is run, always run `idmConfigTool` from the directory:

  ```
  IAM_ORACLE_HOME/idmtools/bin
  ```

- Log File

  You can specify a log file using the `log_file` attribute of idmConfigTool.

  If you do not explicitly specify a log file, a file named `automation.log` is created in the directory where you run the tool.

  Check the log file for any errors or warnings and correct them.

C.3.4 Using the Properties File for idmConfigTool

This section describes the properties file that can be used with idmConfigTool.

- About the idmConfigTool properties File
- List of idmConfigTool Properties

C.3.4.1 About the idmConfigTool properties File

A properties file provides a convenient way to specify command properties and enable you to save properties for reference and later use. You can specify a properties file, containing execution properties, as input command options. The properties file is a simple text file which must be available at the time the command is executed.

For security you are advised not to insert passwords into the properties file. The tool prompts you for the relevant passwords at execution.

C.3.4.2 List of idmConfigTool Properties

Table C-2 lists the properties used by integration command options in the idmConfigTool command. The properties are listed in alphabetical order.

> **WARNING:**
>
> For security, do not put password values in your properties files. idmConfigTool prompts for passwords upon execution.

Table C-2 Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
ACCESS_GATE_ID	IdentityManagerAccessGate	The Access Manager access gate ID with which Oracle Identity Management needs to communicate.
ACCESS_SERVER_HOST	mynode.us.example.com	Access Manager Access Server host name
ACCESS_SERVER_PORT	5575	Access Manager NAP port.
APNS_FILE	/scratch/silent_omsm/keystores/APNS.p12	Apple Push Notification Service (APNS) keystore file; used to establish secure connection to Apple server to send notifications.
APNS_KEYSTORE_PASSWD		APNS keystore password.
APPLE_CACERT_FILE	/scratch/omss/keystores/applerootca.crt	File location of Apple root CA. Required during iOS device enrollment in Oracle Mobile Security Suite (OMSS).
AUTOLOGINURI	/obrar.cgi	URI required by Oracle Platform Security Services (OPSS). Default value is /obrar.cgi
COOKIE_DOMAIN	.us.example.com	Web domain on which the Oracle Identity Management application resides. Specify the domain in the format .cc.example.com.

Table C-2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
COOKIE_EXPIRY_INTERVAL	-1	Cookie expiration period. Set to -1 to denote that the cookie expires when the session is closed.
DB_PASSWD		Database password, used in conjunction with JDCB_URL.
DOMAIN_LOCATION	ORACLE_BASE /admin/IDMDomain/aserver/IDMDomain	The location of the Oracle Identity Governance domain (and OMSM, if applicable).
DOMAIN_NAME	IDM_Domain	The Oracle Identity Governance domain name.
EMAIL_ADMIN_USER	admin@example.com	E-mail admin user; must be an e-mail address.
EMAIL_ADMIN_PASSWD		Email admin user's password
EXCHANGE_DOMAIN_NAME	example.com	Domain name of the exchange server.
EXCHANGE_SERVER_URL	http://testuri.com	URL of the exchange server.
EXCHANGE_LISTENER_URL	http://testuri.com	URL of the exchange listener.
EXCHANGE_SERVER_VERSION	2.0	The version of the exchange server.
EXCHANGE_ADMIN_USER	serviceuser	Admin user of the exchange server.
EXCHANGE_ADMIN_PASSWD		Password of the exchange server's admin user.
GCM_API_KEY	AIzaSyCh_JALj5Y	GCM notification API key.
GCM_SENDER_ID	6.10046E+11	GCM notification sender ID.
IDSTORE_ADMIN_PORT	4444	The admin port for an Oracle Unified Directory (OUD) identity store. idmConfigTool needs to connect on the OUD admin port for all operations changing OUD configuration structures: • creation of global ACIs • creation of indexes
IDSTORE_HOST	idstore.example.com	Host name of the LDAP identity store directory (corresponding to the IDSTORE_DIRECTORYTYPE). If your identity store is in Oracle Internet Directory or Oracle Unified Directory, then IDSTORE_HOST points directly to the Oracle Internet Directory or Oracle Unified Directory host. If the Identity Store is fronted by Oracle Virtual Directory, then IDSTORE_HOST points to the Oracle Virtual Directory host, which is IDSTORE.*example*.com.
IDSTORE_PORT	1389	Port number of the LDAP identity store (corresponding to the IDSTORE_DIRECTORYTYPE).
IDSTORE_BINDDN	cn=orcladmin	Administrative user in the identity store directory.

Table C-2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
IDSTORE_USERNAMEATTRIBUTE	cn	Username attribute used to set and search for users in the identity store. Set to part of the user DN. For example, if the user DN is cn=orcladmin,cn=Users,dc=us,dc=example,dc=com, this property is set to cn.
IDSTORE_LOGINATTRIBUTE	uid or email	Login attribute of the identity store which contains the user's login name. This is the attribute the user uses for login.
IDSTORE_USERSEARCHBASE	cn=Users,dc=us,dc=example,dc=com	Location in the directory where users are stored. This property tells the directory where to search for users.
IDSTORE_SEARCHBASE	dc=us,dc=example,dc=com	Search base for users and groups contained in the identity store. Parent location that contains the USERSEARCHBASE and the GROUPSEARCHBASE. For example: IDSTORE_SEARCHBASE: cn=oracleAccounts,dc=example,dc=com IDSTORE_USERSEARCHBASE: cn=Users,cn=oracleAccounts,dc=example,dc=com IDSTORE_GROUPSEARCHBASE: cn=Groups,cn=oracleAccounts,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE	cn=Groups,dc=us,dc=example,dc=com	The location in the directory where groups (or *roles*) are stored. This property tells the directory where to search for groups or roles.
IDSTORE_OAMSOFTWAREUSER	oamLDAP	The username used to establish the Access Manager identity store connection. This user is created by the idmconfigtool.
IDSTORE_OAMADMINUSER	oamadmin	The identity store administrator you want to create for Access Manager. Required only if the identity store is set as the system identity store. The administrator is created by the idmconfigtool.
IDSTORE_OAAMADMINUSER	oaamadmin	The identity store administrator for Oracle Adaptive Access Manager.
IDSTORE_PROFILENAME	idsprofile	Name of the identity store profile.
IDSTORE_SYSTEMIDBASE	cn=system, dc=test	Location of a container in the directory where system operations users are stored so that they are kept separate from enterprise users stored in the main user container. There are only a few system operations users. One example is the Oracle Identity Management reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.
IDSTORE_READONLYUSER		User with read-only permissions to the identity store.

Table C-2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
IDSTORE_READWRITEUSER		User with read-write permissions to the identity store.
IDSTORE_SUPERUSER		The Oracle Fusion Applications superuser in the identity store.
IDSTORE_XELSYSADMINUSER		The administrator of the xelsysadm system account.
IDSTORE_OIMADMINUSER		The identity store administrator for Oracle Identity Governance. User that Oracle Identity Governance uses to connect to the identity store
IDSTORE_OIMADMINGROUP		The Oracle Identity Governance administrator group you want to create to hold your Oracle Identity Governance administrative users.
IDSTORE_SSL_ENABLED		Whether SSL to the identity store is enabled. Valid values: true | false
IDSTORE_KEYSTORE_FILE	OUD_ORACLE_INSTANCE /OUD /config/admin-keystore	Location of the keystore file containing identity store credentials. Applies to and required for Oracle Unified Directory identity stores.
IDSTORE_KEYSTORE_PASSWORD	4VYGtJLG61V5OjDWKe94e601x7tgLFs	Password of the identity store directory administrator. Not plain-text. Applies to and required for Oracle Unified Directory identity stores. This value can be found in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.
IDSTORE_NEW_SETUP		Used for identity store validation. Used in Oracle Fusion Applications environment.
IDSTORE_DIRECTORYTYPE	OVD	Directory type of the identity store for which the authenticator must be created. Set to OVD if you are using Oracle Virtual Directory server to connect to either a non-OID directory, Oracle Internet Directory or Oracle Unified Directory. Set it to OID if your identity store is in Oracle Internet Directory and you are accessing it directly rather than through Oracle Virtual Directory. Set to OUD if your identity store is Oracle Unified Directory and you are accessing it directly rather than through Oracle Virtual Directory. Valid values: OID, OVD, OUD, AD
IDSTORE_ADMIN_USER	cn=systemids,dc=example,dc=com	The administrator of the identity store directory. Provide the complete LDAP DN of the same user specified for IDSTORE_OAMSOFTWAREUSER. The username alone is not sufficient.
IDSTORE_WLSADMINUSER	weblogic_idm	The identity store administrator for Oracle WebLogic Server; usually weblogic_idm.

Table C-2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
IDSTORE_WLSADMINUSER_PWD		The password of the identity store administrator for Oracle WebLogic Server.
IDSTORE_WLSADMINGROUP	WLS Administrators	The identity store administrator group for Oracle WebLogic Server.
IDSTORE_WASADMINUSER		The "wasadmin" user (IBM WebSphere).
JDBC_URL	jdbc:oracle:thin:@example.com:5521:msmdb	JDBC URL used to seed APNS/GCM data.
LDAPn_HOST	.	The host name of the LDAP server
LDAPn_PORT		The LDAP server port number.
LDAPn_BINDDN	.	The bind DN for the LDAP server
LDAPn_SSL		Indicates whether the connection to the LDAP server is over SSL. Valid values are True or False
LDAPn_BASE		The base DN of the LDAP server.
LDAPn_OVD_BASE		The OVD base DN of the LDAP server.
LDAPn_TYPE		The directory type for the LDAP server. n is 1, 2, and so on. For a single-node configuration specify LDAP1.
LOGINURI	/${app.context}/adfAuthentication	URI required by OPSS. Default value is /${app.context}/adfAuthentication
LOGOUTURI	/oamsso/logout.html	URI required by OPSS. Default value is /oamsso/logout.html
MDS_DB_URL	jdbc:oracle:thin:@DBHOST:1521:SID	URL of the MDS database. It represents a single instance database. The string following the '@' symbol must have the correct values for your environment. SID must be the actual SID, *not* a service name. If you are using a single instance database, then set MDS_URL to: `jdbc:oracle:thin:@DBHOST:1521:SID`.
MDS_DB_SCHEMA_USERNAME	edg_mds	Username of the MDS schema user. MDS schema which Oracle Identity Governance is using.
MSM_SCHEMA_USER	DEV87_OMSM	Mobile Security Manager (MSM) database schema username.
MSM_SERVER_KEY_LENGTH	2048	Key length for the self-signed CA and generated keys for the MSM server. Defaults to 2048.
MSM_SERVER_NAME	omsm_server1	Name of the MSM server. Provide this only if the MSM server is renamed to a different value during domain configuration.
MSAS_SERVER_HOST	server1.example.com	MSAS server host name.
MSAS_SERVER_PORT	11001	MSAS server's SSL port.
OAM_SERVER_VERSION	12c	Valid value is 12c

Table C-2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
OAM_TRANSFER_MODE	SIMPLE	The transfer mode for the Access Manager agent being configured. If your access manager servers are configured to accept requests using the simple mode, set OAM_TRANSFER_MODE to SIMPLE. Valid values are OPEN, SIMPLE or CERT.
OAM11G_OAM_SERVER_TRANSFER_MODE	OPEN	The security model in which the Access Manager 11*g* server functions. Valid values: OPEN or SIMPLE.
OAM11G_SSO_ONLY_FLAG	false	Configures Access Manager 11*g* as authentication only mode or normal mode, which supports authentication and authorization. Default value is `true` (OAM performs no authorization). If set to`true`, the Access Manager 11*g* server operates in authentication only mode, where all authorizations return `true` by default without any policy validations. In this mode, the server does not have the overhead of authorization handling. This is recommended for applications which do not depend on authorization policies and need only the authentication feature of the Access Manager server. If the value is `false`, the server runs in default mode, where each authentication is followed by one or more authorization requests to the OAM Server. WebGate allows the access to the requested resources or not, based on the responses from the OAM server.
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	OAMAdministrators	Name of the group that is used to allow access to the Oracle Access Management Console to administer role security in identity store.
OAM11G_OIM_INTEGRATION_REQ	false	Specifies whether to integrate with Oracle Identity Governance or configure Access Manager in stand-alone mode. Set to `true` for integration. Valid values: true (integration) | false
OAM11G_SERVER_LBR_HOST	sso.example.com	Host name of the load balancer to the Oracle HTTP (OHS) server front-ending the Access Manager server. This and the following two parameters are used to construct your login URL.
OAM11G_SERVER_LBR_PORT	443	Port number of the load balancer to the OHS server front-ending the Access Manager server.
OAM11G_SERVER_LBR_PROTOCOL	https	Protocol of the load balancer to the OHS server front-ending the Access Manager server. Valid values: HTTP, HTTPS
OAM11G_SERVER_LOGIN_ATTRIBUTE	uid	At a login attempt, the username is validated against this attribute in the identity store. Setting to `uid` ensures that when users log in their username is validated against the `uid` attribute in LDAP.

Table C-2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
OAM11G_SERVER_GLOBAL_SESSION_TIMEOUT		The global session timeout for sessions in the Access Manager server.
OAM11G_SERVER_GLOBAL_SESSION_EXPIRY_TIME		Global session expiry time for a session in the Access Manager server.
OAM11G_SERVER_GLOBAL_MAX_SESSION_PER_USER		Global maximum sessions per user in the Access Manager server.
OAM11G_IDSTORE_NAME		The identity store name. If you already have an identity Store in place which you wish to reuse (rather than allowing the tool to create a new one for you), set this parameter to the name of the Identity Store. The default value is "OAMIDStore".
OAM11G_IMPERSONATION_FLAG		Enable or disable impersonation in Access Manager server. Applicable to Oracle Fusion Applications environment. Valid values: true (enable) | false The default is false. If you are using impersonalization, you must manually set this value to true.
OAM11G_IDM_DOMAIN_OHS_HOST	sso.example.com	Host name of the load balancer which is in front of OHS in a high-availability configuration.
OAM11G_IDM_DOMAIN_OHS_PORT	443	Port number on which the load balancer specified as OAM11G_IDM_DOMAIN_OHS_HOST listens.
OAM11G_IDM_DOMAIN_OHS_PROTOCOL	https	Protocol for IDM OHS. Protocol to use when directing requests to the load balancer. Valid values: HTTP | HTTPS
OAM11G_OIM_OHS_URL	https://sso.example.com:443/test	URL of the load balancer or OHS fronting the OIG server.
OAM11G_WG_DENY_ON_NOT_PROTECTED	true	Deny on protected flag for 10g webgate Valid values: true | false
OAM11G_OAM_SERVER_TRANSFER_MODE	simple	Transfer mode for the IDM domain agent. Valid values: OPEN | SIMPLE | CERT
OAM11G_IDM_DOMAIN_LOGOUT_URLS	/console/jsp/common/logout.jsp,/em/targetauth/emaslogout.jsp	Comma-separated list of Access Manager logout URLs.
OAM11G_WLS_ADMIN_HOST	myhost.example.com	On WebLogic Server: Host name of the Access Manager domain admin server. On IBM WebSphere: The Access Manager application server host.
OAM11G_WLS_ADMIN_PORT	7001	On WebLogic Server: Port on which the Access Manager domain admin server is running. On IBM WebSphere: Deployment Manager bootstrap port for Access Manager cell.

Table C-2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
OAM11G_WLS_ADMIN_USER	wlsadmin, wasadmin	On WebLogic Server: The username of the Access Manager domain administrator. On IBM WebSphere: Primary administrative user name for Access Manager cell.
OAM_ADMIN_WAS_DEFAULT_PORT	1443	On IBM WebSphere, OAM node's OracleAdminServer default port number
OAM_POLICY_MGR_SERVER_NAME	oam_policy_mgr1	Name of the Access Manager policy manager server. Provide this only if the policy manager server is renamed to a different value during domain configuration.
OIM_DB_URL		The URL needed to connect to the Oracle Identity Management database.
OIM_DB_SCHEMA_USERNAME		The schema user for the Oracle Identity Management database.
OIM_FRONT_END_HOST	host123.example.com	The host name of the LBR server front-ending Oracle Identity Governance.
OIM_FRONT_END_PORT	7011	The port number of the LBR server front-ending Oracle Identity Governance.
OIM_MANAGED_SERVER_NAME	WLS_OIM1	The name of the Oracle Identity Governance managed server. If clustered, any of the managed servers can be specified.
OIM_MANAGED_SERVER_HOST		The host name of the Oracle Identity Governance managed server.
OIM_MANAGED_SERVER_PORT		The port number of the Oracle Identity Governance managed server.
OIM_MSM_REST_SERVER_URL	https://msm.example.com:1234/	The URL of the Oracle Mobile Security Manager server. Required only if MSM URL needs to be seeded in Oracle Identity Governance and the system property OMSS Enabled set. OIM_MSM_REST_SERVER_URL enables the Mobile Security Manager task flows in the Oracle Identity Governance console. If not set, configOIM will continue the configuration without configuring the Mobile Security Manager. The prerequisite for OMSS Enabled is that the Oracle Identity Governance server should be up.
OIM_T3_HOST		The host name for the Oracle Identity Governance T3 server.
OIM_T3_PORT		The port number of the Oracle Identity Governance T3 server.
OIM_WAS_CELL_CONFIG_DIR		The location of the `fmwconfig` directory within the Oracle Identity Management cell on IBM WebSphere.
OMSS_KEYSTORE_PASSWORD		Password used to generate OMSM keystores and keys

Table C-2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
OMSM_IDSTORE_ROLE_SECURITY_ADMIN	MSMAdmin	Name of the admin group whose members have admin privileges for OMSM operations. Default is "IDM Administrators".
OMSM_IDSTORE_ROLE_SECURITY_HELPDESK	MSMHelpDeskUsers	Name of the msm helpdesk group, whose members get helpdesk privileges for OMSM operations. Default is "MSMHelpdeskUsers".
ovd.host		OVD Server host name
ovd.port		OVD Server port number
ovd.binddn		OVD Server bind DN
ovd.ssl		Indicates whether the connection is over SSL. Valid values are True or False
ovd.oamenabled		Indicates whether Oracle Access Manager is enabled. Valid values are True or False
POLICYSTORE_SHARES_IDSTORE	true	Denotes whether the policy store and identity store share the directory. Always `true` in Release 11*g*. Valid values: true, false
POLICYSTORE_HOST	mynode.us.example.com	The host name of your policy store directory.
POLICYSTORE_PORT	1234	The port number of your policy store directory.
POLICYSTORE_BINDDN	cn=orcladmin	Administrative user in the policy store directory.
POLICYSTORE_SEARCHBASE	dc=example,dc=com	The location in the directory where users and groups are stored.
POLICYSTORE_SYSTEMIDBASE	cn=systemids, dc=example,dc=com	The read-only and read-write users for policy store are created in this location. Default value is cn=systemids, `policy_store_search_base`
POLICYSTORE_READONLYUSER	PolStoreROUser	A user with read privileges in the policy store.
POLICYSTORE_READWRITEUSER	PolStoreRWUser	A user with read and write privileges in the policy store.
POLICYSTORE_CONTAINER	cn=jpsroot	The name of the container used for OPSS policy information
POLICYSTORE_SSL_ENABLED		Whether the policy store is SSL-enabled.
POLICYSTORE_KEYSTORE_FILE		The location of the keystore file for an SSL-enabled policy store.
PROXY_SERVER_HOST	www-proxy.example.com	Proxy server's host name.
PROXY_SERVER_PORT	80	Proxy server's port.
PROXY_USER	proxyuserA	User for proxy.
PROXY_PASSWD		Password for proxy user.

Table C-2 (Cont.) Properties Used in IdMConfigtool properties Files

Parameter	Example Value	Description
SCEP_DYNAMIC_CHALLENGE_USER		OMSM uses a Simple Certificate Enrollment Protocol (SCEP) dynamic challenge for external SCEP authentication during the enrollment phase. This user account is used for authentication.
SCEP_DYNAMIC_CHALLENGE_PASSWD		SCEP dynamic challenge user's password
SPLIT_DOMAIN	true	Flag to force `configOAM` to create security providers in the domain against which it is run. Valid values are true, false. Setting to true is required to suppress the double authentication of Oracle Access Management Console in a split domain scenario.
SSO_ENABLED_FLAG	false	Flag to determine if SSO should be enabled. Valid values are true, false.
WEBGATE_TYPE	`javaWebgate`	The type of WebGate agent you want to create. Set to `ohsWebgate12c`.
PRIMARY_OAM_SERVERS	idmhost1.example.com:5575,idmhost2.example.com:5575	A comma-separated list of your Access Manager servers and their proxy ports. To determine the proxy ports your Access Manager servers: 1. Log in to the Oracle Access Management Console at `http://admin.example.com:7001/oamconsole` 2. At the top of the Oracle Access Management Console, click **Configuration**. 3. In the Configuration console, click **Server Instances**. 4. In the page that appears, click **Search**, then double-click the target instance to display its configuration. For example, WLS_OAM1. The proxy port is shown as **Port**.
SMTP_HOST	exchangeurl.us.example.com	E-mail host.
SMTP_PORT	80	E-mail port.
TOPIC	com.apple.mgmt.External.2544264e-aa8a-4654-bfff-9d897ed39a87	Topic used in Apple's APNS certificate; used to send APNS notification. The value should match the UID of the APNS key.
USE_PROXY	true	Indicates whether to use a proxy. Valid values are true, false.
WLSHOST	`node01.example.com`	WebLogic Server host name (host name of your administration server).
WLSPORT	7001	The WebLogic Server port number
WLSADMIN	wlsadmin	The administrator login, depending on the application server context.
WLSPASSWD		The WebLogic Server administrator password.

C.3.5 Working with the idmConfigTool Log File

`idmConfigTool` logs execution details to a file called `automation.log`, which is helpful in verifying the results of a run.

- Searching the idmConfigTool Log File
- Maintaining the idmConfigTool Log File

C.3.5.1 Searching the idmConfigTool Log File

The log file contains initialization and informational messages:

```
Feb 18, 2015 8:38:14 PM oracle.idm.automation.util.Util setLogger
WARNING: Logger initialized in warning mode
Feb 18, 2015 8:38:19 PM
oracle.idm.automation.impl.oim.handlers.OIMPreIntegrationHandler <init>
INFO: Appserver type: null
Feb 18, 2015 8:38:20 PM
oracle.idm.automation.impl.oim.handlers.OIMPreIntegrationHandler <init>
WARNING: Cannot connect to the OUD Admin connector
Feb 18, 2015 8:38:29 PM
oracle.idm.automation.impl.oim.handlers.OIMPreIntegrationHandler
createOIMAdminUser
INFO: OIM Admin User has been created
Feb 18, 2015 8:38:29 PM
oracle.idm.automation.impl.oim.handlers.OIMPreIntegrationHandler
addPwdResetPrivilegeToOIMAdminUser
INFO: Password reset privilege added
```

Checking for `WARNING` messages after a run can help you identify potential problems with the run.

C.3.5.2 Maintaining the idmConfigTool Log File

`idmConfigTool` appends to the log file upon each run. The presence of older entries can lead to a misunderstanding if you see an error in the log and correct it, since the original error detail is present in the log even after you rectify the error.

> **WARNING:**
>
> Back up existing log files frequently to avoid confusion caused by old log entries.

C.4 Additional Tasks for OUD Identity Store in an HA Environment

This section explains additional tasks you may need to perform when using `idmConfigTool` for a target Oracle Unified Directory (OUD) identity store in a high-availability environment. Topics include:

- Creating the Global ACI for Oracle Unified Directory

- Creating Indexes on Oracle Unified Directory Replicas

C.4.1 Creating the Global ACI for Oracle Unified Directory

Global ACI and indexes are not replicated when you use `idmConfigTool` for an Oracle Unified Directory (OUD) identity store in a high availability (HA) environment that contains replicas. Global ACI and indexes are created ONLY in the instance(s) specified in the property file. You must manually re-create (remove then create) them on all other OUD instances of the replication domain.

Consequently you must first grant access to the change log, and then create the ACIs. Take these steps:

1. Create a file called `password` which contains the password you use to connect to OUD.
2. Remove the existing change log on one of the replicated OUD hosts. The command syntax is:

```
OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--remove \
global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version 3.0;
acl \"External changelog access\"; deny (all) userdn=\"ldap:///anyone\";)"
--hostname OUD Host \
--port OUD Admin Port \
--trustAll ORACLE_INSTANCE/config/admin-truststore \
--bindDN cn=oudadmin \
--bindPasswordFile password \
--no-prompt
```

   For example:

```
OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--remove
global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version 3.0;
acl \"External changelog access\"; deny (all) userdn=\"ldap:///anyone\";)"
--hostname OUDHOST1.example.com \
--port 4444 \
--trustAll /u01/app/oracle/admin/oud1/OUD/config/admin-truststore \
--bindDN cn=oudadmin \
--bindPasswordFile password \
--no-prompt
```

3. Add the new ACI for the changelog:

```
OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version
3.0; acl \"External changelog access\"; allow
(read,search,compare,add,write,delete,export)
groupdn=\"ldap:///cn=oimAdminGroup,cn=groups,dc=example,dc=com\";)" \
--hostname OUD Host \
--port OUD Admin Port \
--trustAll \
--bindDN cn=oudadmin \
--bindPasswordFile password
--no-prompt
```

   For example:

```
OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add
--add global-aci:"(target=\"ldap:///cn=changelog\")(targetattr=\"*\")(version
```

```
3.0; acl \"External changelog access\"; allow
(read,search,compare,add,write,delete,export)
groupdn=\"ldap:///cn=oimAdminGroup,cn=groups,dc=example,dc=com\";)" \
--hostname OUDHOST1 \
--port 4444 \
--trustAll \
--bindDN cn=oudadmin \
--bindPasswordFile password
--no-prompt
```

4. Then add the ACI:

```
OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add global-aci:"(targetcontrol=\"1.3.6.1.4.1.26027.1.5.4 ||
1.3.6.1.4.1.26027.2.3.4\")(version 3.0; acl \"OIMAdministrators control
access\"; allow(read)  groupdn=\"<ldap:///
cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com\";)" \
        --hostname OUD_HOST \
        --port OUD_ADMIN_PORT \
        --trustAll \
        --bindDN cn=oudadmin \
        --bindPasswordFile passwordfile \
        --no-prompt
```

For example:

```
OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add global-aci:"(targetcontrol=\"1.3.6.1.4.1.26027.1.5.4 ||
1.3.6.1.4.1.26027.2.3.4\")(version 3.0; acl \"OIMAdministrators control
access\"; allow(read) groupdn=\"ldap:///
cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com\";)" \
        --hostname IDMHOST1.mycompany.com \
        --port 4444 \
        --trustAll \
        --bindDN cn=oudadmin \
        --bindPasswordFile passwordfile \
        --no-prompt
```

5. Finally add the ACI:

```
OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add global-aci:"(target=\"ldap:///\")(targetscope=\"base\")
(targetattr=\"lastExternalChangelogCookie\")(version 3.0; acl \"User-Visible
lastExternalChangelog\"; allow (read,search,compare) groupdn=\"ldap:///
cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com\";)" \
        --hostname OUD_HOST \
        --port OUD_ADMIN_PORT \
        --trustAll \
        --bindDN cn=oudadmin \
        --bindPasswordFile passwordfile \
        --no-prompt
```

For example:

```
OUD_ORACLE_INSTANCE/bin/dsconfig set-access-control-handler-prop \
--add global-aci:"(target=\"ldap:///\")(targetscope=\"base\")
(targetattr=\"lastExternalChangelogCookie\")(version 3.0; acl \"User-Visible
lastExternalChangelog\"; allow (read,search,compare) groupdn=\"ldap:///
cn=OIMAdministrators,cn=groups,dc=mycompany,dc=com\";)" \
        --hostname IDMHOST1.mycompany.com \
        --port 4444 \
        --trustAll \
        --bindDN cn=oudadmin \
```

```
--bindPasswordFile passwordfile \
--no-prompt
```

6. Repeat Steps 1 through 5 for each OUD instance.

C.4.2 Creating Indexes on Oracle Unified Directory Replicas

When `idmConfigTool` prepares the identity store, it creates a number of indexes on the data. However in a high availability (HA) environment that contains replicas, global ACI and indexes are created only in the instance(s) specified in the property file; the replicas are not updated with the indexes which need to be added manually.

The steps are as follows (with `LDAPHOST1.example.com` representing the first OUD server, `LDAPHOST2.example.com` the second server, and so on):

1. Create a file called `password` which contains the password you use to connect to OUD.
2. Configure the indexes on the second OUD server:

```
ORACLE_INSTANCE/OUD/bin/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444
-a -D "cn=oudadmin" -j password -c -f
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/ldif/ojd/schema/
ojd_user_index_generic.ldif
```

and

```
ORACLE_INSTANCE/OUD/bin/ldapmodify -h LDAPHOST2.example.com -Z -X -p 4444
-a -D "cn=oudadmin" -j  password -c -f
/u01/app/oracle/product/fmw/iam/idmtools/templates/oud/oud_indexes_extn.ldif
```

> **Note:**
>
> - Repeat both commands for all OUD servers for which idmConfigTool was not run.
> - Execute the commands on one OUD instance at a time; that instance must be shut down while the commands are running.

3. Rebuild the indexes on all the servers:

```
ORACLE_INSTANCE/OUD/bin/bin/rebuild-index -h localhost -p 4444 -X -D
"cn=oudadmin" -j password --rebuildAll -b "dc=example,dc=com"
```

> **Note:**
>
> You must run this command on all OUD servers, including the first server (`LDAPHOST1.example.com`) for which `idmConfigTool` was run.

C.5 IdmConfigTool Options and Properties

This section lists the properties for each command option. Topics include:

- preConfigIDStore Command

- prepareIDStore Command
- configOAM Command

> **Note:**
>
> - The command options show the command syntax on Linux only. See idmConfigTool Command Syntax for Windows syntax guidelines.
> - The tool prompts for passwords.

C.6.1 preConfigIDStore Command

Syntax

On Linux, the command syntax is:

```
idmConfigTool.sh -preConfigIDStore input_file=input_properties
```

On Windows, the command syntax is:

```
idmConfigTool.bat -preConfigIDStore input_file=input_properties
```

For example:

```
idmConfigTool.sh -preConfigIDStore input_file=extendOAMPropertyFile
```

> **Note:**
>
> The `-preConfigIDStore` command option supports Oracle Internet Directory, Oracle Unified Directory, and Oracle Virtual Directory.

Properties

Table C-3 lists the properties for this mode:

Table C-3 Properties of preConfigIDStore

Property	Required?
`IDSTORE_HOST`	`YES` `IDSTORE_HOST` and `IDSTORE_PORT` are the host and port, respectively, of your identity store directory. If your identity store is in Oracle Unified Directory or Oracle Internet Directory, then `IDSTORE_HOST` should point directly to the Oracle Unified Directory or Oracle Internet Directory host. If your Identity Store is fronted by Oracle Virtual Directory, then IDSTORE_HOST should point to the Oracle Virtual Directory host, which should be `IDSTORE.example.com`.
`IDSTORE_PORT`	`YES`

Table C-3 (Cont.) Properties of preConfigIDStore

Property	Required?
IDSTORE_BINDDN	YES
IDSTORE_DIRECTORYTYPE	YES (if target identity store is an instance of Oracle Unified Directory (OUD).)
IDSTORE_LOGINATTRIBUTE	
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_SYSTEMIDBASE	
POLICYSTORE_SHARES_IDSTORE	
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).) This property is required to connect to and configure OUD configuration structures: • creation of global ACIs • creation of indexes
IDSTORE_KEYSTORE_FILE	YES, if target identity store is OUD. Use the format: *OUD-instance-path*/OUD/config/admin-keystore where *OUD-instance-path* is the path to the directory instance. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.

Example properties File

Here is a sample properties file for this option:

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

If you are using Oracle Unified Directory as the identity store, include the additional properties indicated in the properties table. The sample properties file then contains the additional properties:

```
IDSTORE_DIRECTORYTYPE: OUD
IDSTORE_ADMIN_PORT : 4444
IDSTORE_KEYSTORE_FILE : /u01/config/instances/oud1/OUD/config/admin-keystore
IDSTORE_KEYSTORE_PASSWORD : K8BYCoOFHBwDYa1F6vUBgcGr1TK1Rz26W9Bz7OF0UwsZ5XLGOb
```

> **Note:**
>
> When using `prepareIDStore` for Oracle Unified Directory, global ACI and indexes are re-created only in the instance(s) specified in the property file; they are not replicated by Oracle Unified Directory. You must manually re-create (remove, then create) the global ACI and indexes on all other Oracle Unified Directory instances of the replication domain.
>
> For details, see Additional Tasks for OUD Identity Store in an HA Environment.

C.6.2 prepareIDStore Command

Syntax

The prepareIDStore command takes `mode` as an argument to perform tasks for the specified component.

```
idmConfigTool.sh -prepareIDStore mode=mode
input_file=filename_with_Configproperties
```

where mode must be one of the following:

- OAM
- OIM
- OAAM
- WLS
- FUSION
- WAS
- APM
- all (performs all the tasks of the above modes combined)

> **Note:**
>
> WLS mode must be run before OAM.

> **See Also:**
>
> Table C-2 for details of the properties.

C.6.2.1 prepareIDStore mode=OAM

The following are created in this mode:

- Perform schema extensions as required by the Access Manager component
- Add the oblix schema
- Create the OAMSoftware User
- Create OblixAnonymous User
- Optionally create the Access Manager Administration User
- Associate these users to their respective groups
- Create the group "orclFAOAMUserWritePrivilegeGroup"

Syntax

On Linux, the command syntax is:

```
idmConfigTool.sh -prepareIDStore mode=OAM input_file=filename_with_Configproperties
```

On Windows, the command syntax is:

```
idmConfigTool.bat -prepareIDStore mode=OAM input_file=filename_with_Configproperties
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=OAM input_file=preconfigOAMPropertyFile
```

Properties

Table C-4 lists the properties for this mode:

Table C-4 prepareIDStore mode=OAM Properties

Parameter	Required?
IDSTORE_HOST	YES IDSTORE_HOST and IDSTORE_PORT are the host and port, respectively, of your Identity Store directory. If your Identity Store is in Oracle Internet Directory or Oracle Unified Directory, then IDSTORE_HOST should point to Oracle Internet Directory or Oracle Unified Directory, even if you are fronting Oracle Internet Directory with Oracle Virtual Directory. If you are using a directory other than Oracle Internet Directory or Oracle Unified Directory, specify the Oracle Virtual Directory host.
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES

Table C-4 (Cont.) prepareIDStore mode=OAM Properties

Parameter	Required?
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_OAMSOFTWAREUSER	
IDSTORE_OAMADMINUSER	
IDSTORE_SYSTEMIDBASE	
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).) This property is required to connect to and configure OUD configuration structures: • creation of global ACIs • creation of indexes
IDSTORE_KEYSTORE_FILE	YES, if target identity store is OUD. Use the format: *OUD-instance-path*/OUD/config/admin-keystore where *OUD-instance-path* is the path to the directory instance. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.

Example properties File

Here is a sample properties file for this option. This parameter set would result in OAMADMINUSER and OAMSOFTWARE user being created in the identity store:

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN:OAMAdministrators
IDSTORE_OAMSOFTWAREUSER:oamLDAP
IDSTORE_OAMADMINUSER:oamadmin
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
```

> **See Also:**
>
> Table C-2 for details of the properties.

C.6.2.2 prepareIDStore mode=OIM

The following are created in this mode:

- Create Oracle Identity Management Administration User under SystemID container
- Create Oracle Identity Management Administration Group
- Add Oracle Identity Management Administration User to Oracle Identity Management Administration Group
- Add ACIs to Oracle Identity Management Administration Group
- Create reserve container
- Create `xelsysadmin` user

Syntax

On Linux, the command syntax is:

```
idmConfigTool.sh -prepareIDStore mode=OIM input_file=filename_with_Configproperties
```

On Windows, the command syntax is:

```
idmConfigTool.bat -prepareIDStore mode=OIM input_file=filename_with_Configproperties
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=OIM input_file=preconfigOIMPropertyFile
```

Properties

Table C-5 lists the properties in this mode:

Table C-5 prepareIDStore mode=OIM Properties

Parameter	Required?
`IDSTORE_HOST`	YES `IDSTORE_HOST` and `IDSTORE_PORT` are the host and port, respectively, of your Identity Store directory. If your Identity Store is in Oracle Internet Directory or Oracle Unified Directory, then `IDSTORE_HOST` should point directly to the Oracle Internet Directory or Oracle Unified Directory host. If your Identity Store is fronted by Oracle Virtual Directory, then `IDSTORE_HOST` should point to the Oracle Virtual Directory host, which should be `IDSTORE.example.com`.
`IDSTORE_PORT`	YES
`IDSTORE_BINDDN`	YES
`IDSTORE_USERNAMEATTRIBUTE`	YES

Table C-5 (Cont.) prepareIDStore mode=OIM Properties

Parameter	Required?
IDSTORE_LOGINATTRIBUTE	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_OIMADMINUSER	
IDSTORE_OIMADMINGROUP	
IDSTORE_SYSTEMIDBASE	
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).) This property is required to connect to and configure OUD configuration structures: • creation of global ACIs • creation of indexes
IDSTORE_KEYSTORE_FILE	YES (if target identity store is an instance of OUD) IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES (if target identity store is an instance of OUD.) Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin..
OIM_DB_URL	Required on IBM WebSphere.
OIM_DB_SCHEMA_USERNAME	Required on IBM WebSphere.
OIM_WAS_CELL_CONFIG_DIR	Required on IBM WebSphere.

Example properties File

Here is a sample properties file for this option:

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE:cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_OIMADMINUSER: oimadmin
IDSTORE_OIMADMINGROUP:OIMAdministrators
OIM_DB_URL: jdbc:oracle:thin:@xyz5678.us.example.com:5522:wasdb1
OIM_DB_SCHEMA_USERNAME: dev_oim
OIM_WAS_CELL_CONFIG_DIR: /wassh/WebSphere/AppServer/profiles/Dmgr04/config/cells/
xyz5678Cell04/fmwconfig
```

> **See Also:**
>
> Table C-2 for details of the properties.

C.6.2.3 prepareIDStore mode=OAAM

This mode:

- Creates Oracle Adaptive Access Manager Administration User
- Creates Oracle Adaptive Access Manager Groups
- Adds the Oracle Adaptive Access Manager Administration User as a member of Oracle Adaptive Access Manager Groups

Syntax

```
idmConfigTool.sh -prepareIDStore mode=OAAM
input_file=filename_with_Configproperties
```

Properties

Table C-6 shows the properties in this mode:

Table C-6 prepareIDStore mode=OAAM Properties

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	YES
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_OAAMADMINUSER	YES
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).) This property is required to connect to and configure OUD configuration structures: • creation of global ACIs • creation of indexes

Table C-6 (Cont.) prepareIDStore mode=OAAM Properties

Parameter	Required?
IDSTORE_KEYSTORE_FILE	YES, if target identity store is OUD. Use the format: *OUD-instance-path*/OUD/config/admin-keystore where *OUD-instance-path* is the path to the directory instance. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.

Example properties File

Here is a sample properties file for this option:

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE:cn=Users,dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_OAAMADMINUSER: oaamadmin
POLICYSTORE_SHARES_IDSTORE: true
```

> **See Also:**
>
> Table C-2 for details of the properties.

C.6.2.4 prepareIDStore mode=WLS

This mode:

- Creates Weblogic Administration User
- Creates Weblogic Administration Group
- Adds the Weblogic Administration User as a member of Weblogic Administration Group

Syntax

On Linux, the command syntax is:

```
idmConfigTool.sh -prepareIDStore mode=WLS
input_file=filename_with_Configproperties
```

On Windows, the command syntax is:

```
idmConfigTool.bat -prepareIDStore mode=WLS input_file=filename_with_Configproperties
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=WLS input_file=preconfigWLSPropertyFile
```

Properties

Table C-7 lists the properties in this mode:

Table C-7 prepareIDStore mode=WLS Properties

Parameter	Required?
IDSTORE_HOST	YES IDSTORE_HOST and IDSTORE_PORT are the host and port, respectively, of your Identity Store directory. If your Identity Store is in Oracle Internet Directory or Oracle Unified Directory, then IDSTORE_HOST should point to the Oracle Internet Directory or Oracle Unified Directory host, even if you are fronting Oracle Internet Directory with Oracle Virtual Directory. If you are using a directory other than Oracle Internet Directory or Oracle Unified Directory, specify the Oracle Virtual Directory host (which should be *IDSTORE*.example.com.)
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	YES
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_WLSADMINUSER	YES. Do not set any default, out-of-the-box users such as weblogic/ xelsysadm for this property.
IDSTORE_WLSADMINGROUP	YES **Note:** IDSTORE_WLSADMINGROUP: IDM Administrators must be included in the properites file to ensure the OAM Administrators are added to the IDM Administrators group successfully.
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).) This property is required to connect to and configure OUD configuration structures: • creation of global ACIs • creation of indexes

Table C-7 (Cont.) prepareIDStore mode=WLS Properties

Parameter	Required?
IDSTORE_KEYSTORE_FILE	YES, if target identity store is OUD. Use the format: *OUD-instance-path*/OUD/config/admin-keystore where *OUD-instance-path* is the path to the OUD instance. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.

Example properties File

Here is a sample properties file for this option. With this set of properties, the IDM Administrators group is created.

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users, dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_WLSADMINUSER: weblogic_idm
IDSTORE_WLSADMINGROUP: wlsadmingroup
```

> **See Also:**
>
> Table C-2 for details of the properties.

C.6.2.5 prepareIDStore mode=WAS

This mode:

- Creates WebSphere Administration User
- Creates WebSphere Administration Group
- Adds the WebSphere Administration User as a member of WebSphere Administration Group

Syntax

```
idmConfigTool.sh -prepareIDStore mode=WAS
input_file=filename_with_Configproperties
```

Properties

Table C-8 lists the properties in this mode:

Table C-8 prepareIDStore mode=WAS Properties

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_WASADMINUSER	YES (wsadmin user)
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD). This property is required to connect to and configure OUD configuration structures: • creation of global ACIs • creation of indexes
IDSTORE_KEYSTORE_FILE	YES, if target identity store is OUD. Use the format: *OUD-instance-path*/OUD/config/admin-keystore where *OUD-instance-path* is the path to the OUD instance. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.

Example properties File

Here is a sample properties file for this option, which creates the IDM Administrators group.

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users, dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_WASADMINUSER: websphere_idm
```

> **See Also:**
>
> Table C-2 for details of the properties.

C.6.2.6 prepareIDStore mode=APM

This mode:

- Creates Oracle Privileged Account Manager Administration User
- Adds the Oracle Privileged Account Manager Administration User as a member of Oracle Privileged Account Manager Groups

You are prompted to enter the password of the account that you are using to connect to the identity store.

Syntax

```
idmConfigTool.sh -prepareIDStore mode=APM
input_file=filename_with_Configproperties
```

Properties

Table C-9 shows the properties in this mode:

Table C-9 prepareIDStore mode=APM Properties

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERNAMEATTRIBUTE	
IDSTORE_LOGINATTRIBUTE	
IDSTORE_USERSEARCHBASE	
IDSTORE_GROUPSEARCHBASE	
IDSTORE_SEARCHBASE	
POLICYSTORE_SHARES_IDSTORE	YES
IDSTORE_APMUSER	YES

Example properties File

Here is a sample properties file for this option:

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

```
POLICYSTORE_SHARES_IDSTORE: true
IDSTORE_APMUSER: opamadmin
```

> **See Also:**
>
> Table C-2 for details of the properties.

C.6.2.7 prepareIDStore mode=fusion

This mode:.

- Creates a `Readonly` User
- Creates a `ReadWrite` User
- Creates a Super User
- Adds the `readOnly` user to the groups `orclFAGroupReadPrivilegeGroup` and `orclFAUserWritePrefsPrivilegeGroup`
- Adds the `readWrite` user to the groups `orclFAUserWritePrivilegeGroup` and `orclFAGroupWritePrivilegeGroup`

Syntax

```
idmConfigTool.sh -prepareIDStore mode=fusion
input_file=filename_with_Configproperties
```

Properties

Table C-10 lists the properties in this mode:

Table C-10 prepareIDStore mode=fusion Properties

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_READONLYUSER	
IDSTORE_READWRITEUSER	
IDSTORE_SUPERUSER	
IDSTORE_SYSTEMIDBASE	
POLICYSTORE_SHARES_IDSTORE	

Table C-10 (Cont.) prepareIDStore mode=fusion Properties

Parameter	Required?
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).) This property is required to connect to and configure OUD configuration structures: • creation of global ACIs • creation of indexes
IDSTORE_KEYSTORE_FILE	YES, if target identity store is OUD. Use the format: *OUD-instance-path*/OUD/config/admin-keystore where *OUD-instance-path* is the path to the OUD instance. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.

Example properties File

Here is a sample properties file for this option, which creates IDSTORE_SUPERUSER:

```
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_READONLYUSER: IDROUser
IDSTORE_READWRITEUSER: IDRWUser
IDSTORE_USERSEARCHBASE:cn=Users,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycomapny,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_SUPERUSER: weblogic_fa
POLICYSTORE_SHARES_IDSTORE: true
```

> **See Also:**
>
> Table C-2 for details of the properties.

C.6.2.8 prepareIDStore mode=all

The mode performs all the tasks that are performed in the modes OAM, OIM, WLS, WAS, OAAM, and FUSION.

Syntax

```
idmConfigTool.sh -prepareIDStore mode=all
input_file=filename_with_Configproperties
```

Properties

Table C-11 lists the properties in this mode:

Table C-11 prepareIDStore mode=all Properties

Parameter	Required?
IDSTORE_HOST	YES
IDSTORE_PORT	YES
IDSTORE_BINDDN	YES
IDSTORE_USERSEARCHBASE	YES
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_LOGINATTRIBUTE	YES
IDSTORE_SEARCHBASE	YES
IDSTORE_SYSTEMIDBASE	
IDSTORE_READONLYUSER	YES
IDSTORE_READWRITEUSER	YES
IDSTORE_SUPERUSER	YES
IDSTORE_OAMSOFTWAREUSER	YES
IDSTORE_OAMADMINUSER	YES
IDSTORE_OIMADMINUSER	YES
IDSTORE_OIMADMINGROUP	YES
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_OAAMADMINUSER	YES
IDSTORE_WLSADMINUSER	YES
IDSTORE_WLSADMINGROUP	YES
IDSTORE_ADMIN_PORT	YES (if target identity store is an instance of Oracle Unified Directory (OUD).) This property is required to connect to and configure OUD configuration structures: • creation of global ACIs • creation of indexes
IDSTORE_KEYSTORE_FILE	YES, if target identity store is OUD. Use the format: *OUD-instance-path*/OUD/config/admin-keystore where *OUD-instance-path* is the path to the OUD instance. IDSTORE_KEYSTORE_FILE and IDSTORE_KEYSTORE_PASSWORD must be set to establish the connection to the OUD identity store.
IDSTORE_KEYSTORE_PASSWORD	YES, if target identity store is OUD. Not plain-text. Resides in the file OUD_ORACLE_INSTANCE/OUD/config/admin-keystore.pin.
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	

Table C-11 (Cont.) prepareIDStore mode=all Properties

Parameter	Required?
POLICYSTORE_SHARES_IDSTORE	
OIM_DB_URL	Required on IBM WebSphere
OIM_DB_SCHEMA_USERNAME	Required on IBM WebSphere
OIM_WAS_CELL_CONFIG_DIR	Required on IBM WebSphere
IDSTORE_WASADMINUSER	Required on IBM WebSphere

Example properties File

Here is a sample properties file for this option:

```
IDSTORE_HOST: node01.example.com
IDSTORE_PORT: 2345
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
IDSTORE_READONLYUSER: IDROUser
IDSTORE_READWRITEUSER: IDRWUser
IDSTORE_SUPERUSER: weblogic_fa
IDSTORE_OAMSOFTWAREUSER:oamSoftwareUser
IDSTORE_OAMADMINUSER:oamAdminUser
IDSTORE_OIMADMINUSER: oimadminuser
POLICYSTORE_SHARES_IDSTORE: true
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN:OAMAdministrators
IDSTORE_OIMADMINGROUP: OIMAdministrators
IDSTORE_WLSADMINUSER: weblogic_idm
IDSTORE_WLSADMINGROUP: wlsadmingroup
IDSTORE_OAAMADMINUSER: oaamAdminUser
OIM_DB_URL: jdbc:oracle:thin:@xyz5678.us.example.com:5522:wasdb1
OIM_DB_SCHEMA_USERNAME: dev_oim
OIM_WAS_CELL_CONFIG_DIR: /wassh/WebSphere/AppServer/profiles/Dmgr04/config/cells/
xyz5678Cell04/fmwconfig
IDSTORE_WASADMINUSER: websphere_idm
```

> **See Also:**
>
> Table C-2 for details of the properties.

C.6.3 configOAM Command

Prerequisite

Ensure that the administration server for the domain hosting Oracle Access Manager is running before you execute this command.

Restart all servers on the OIM domain after running `configOIM`.

Syntax

On Linux, the command syntax is:

```
idmConfigTool.sh -configOAM input_file=input_properties
```

On Windows, the command syntax is:

```
idmConfigTool.bat -configOAM input_file=input_properties
```

For example:

```
idmConfigTool.sh -configOAM input_file=OAMconfigPropertyFile
```

Properties

Table C-12 lists the command properties.

Table C-12 Properties of configOAM

Property	Required?
WLSHOST	YES WLSHOST and WLSPORT are, respectively, the host and port of your administration server, this will be the virtual name.
WLSPORT	YES
WLSADMIN	YES
IDSTORE_BINDDN	YES
IDSTORE_HOST	YES IDSTORE_HOST and IDSTORE _PORT are, respectively, the host and port of your Identity Store directory. If using a directory server other than Oracle Internet Directory or Oracle Unified Directory, specify the Oracle Virtual Directory host and port.
IDSTORE_PORT	YES
IDSTORE_DIRECTORYTYPE	YES
IDSTORE_BINDDN	YES IDSTORE_BINDDN is an administrative user in Oracle Internet Directory or Oracle Unified Directory. If using a directory server other than Oracle Internet Directory or Oracle Unified Directory, specify an Oracle Virtual Directory administrative user.
IDSTORE_USERNAMEATTRIBUTE	YES
IDSTORE_LOGINATTRIBUTE	YES
IDSTORE_USERSEARCHBASE	YES
IDSTORE_SEARCHBASE	YES

Table C-12 (Cont.) Properties of configOAM

Property	Required?
IDSTORE_GROUPSEARCHBASE	YES
IDSTORE_OAMSOFTWAREUSER	YES
IDSTORE_OAMADMINUSER	YES
IDSTORE_SYSTEMIDBASE	YES
PRIMARY_OAM_SERVERS	YES
WEBGATE_TYPE	YES WEBGATE_TYPE is the type of WebGate agent you want to create. Valid value is ohsWebgate12c
ACCESS_GATE_ID	YES ACCESS_GATE_ID is the name you want to assign to the WebGate. Do *not* change the property value shown in the example.
OAM_TRANSFER_MODE	YES Default is OPEN OAM_TRANSFER_MODE is the security model in which the access servers function.
COOKIE_DOMAIN	YES
COOKIE_EXPIRY_INTERVAL	YES
OAM11G_WG_DENY_ON_NOT_PROTECTED	YES
OAM11G_IDM_DOMAIN_OHS_HOST	YES
OAM11G_IDM_DOMAIN_OHS_PORT	YES
OAM11G_IDM_DOMAIN_OHS_PROTOCOL	YES default is http OAM11G_IDM_DOMAIN_OHS_PROTOCOL is the protocol to use when directing requests to the load balancer.
OAM11G_OAM_SERVER_TRANSFER_MODE	YES OAM11G_OAM_SERVER_TRANSFER_MODE is the security model for the Access Manager servers. Access Manager must be configured for SIMPLE as the mode of communication.
OAM11G_IDM_DOMAIN_LOGOUT_URLS	
OAM11G_OIM_WEBGATE_PASSWD	YES
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN	YES

Table C-12 (Cont.) Properties of configOAM

Property	Required?
OAM11G_SSO_ONLY_FLAG	YES Default is TRUE OAM11G_SSO_ONLY_FLAG configures Access Manager 11*g* as authentication only mode or normal mode, which supports authentication and authorization. Default value is true. If OAM11G_SSO_ONLY_FLAG is true, the Access Manager 11*g* server operates in authentication only mode, where all authorizations return true by default without any policy validations. In this mode, the server does not have the overhead of authorization handling. This is recommended for applications which do not depend on authorization policies and need only the authentication feature of the Access Manager server. If the value is false, the server runs in default mode, where each authentication is followed by one or more authorization requests to the Access Manager server. WebGate allows the access to the requested resources or not, based on the responses from the Access Manager server.
OAM11G_OIM_INTEGRATION_REQ	YES
OAM11G_IMPERSONATION_FLAG	YES OAM11G_IMPERSONATION_FLAG enables or disables the impersonation feature in the OAM Server. Valid values are true (enable) and false (disable). The default is false. If you are using impersonalization, you must manually set this value to true.
OAM11G_SERVER_LBR_HOST	YES
OAM11G_SERVER_LBR_PORT	YES
OAM11G_SERVER_LBR_PROTOCOL	YES Default is http OAM11G_SERVER_LBR_PROTOCOL is the URL prefix to use.
OAM11G_SERVER_LOGIN_ATTRIBUTE	YES
OAM11G_IDSTORE_NAME	YES
POLICYSTORE_SHARES_IDSTORE	YES
OAM11G_OIM_OHS_URL	http://*sso.example.com*:443/ OAM11G_OIM_OHS_URL is the URL of the load balancer or OHS fronting the OIM server.

Table C-12 (Cont.) Properties of configOAM

Property	Required?
SPLIT_DOMAIN	Set to true for cross-domain deployment. Omit for single-domain deployment. SPLIT_DOMAIN set to true is required to suppress the double authentication of Oracle Access Management Console in a split domain scenario.

Example properties File

Here is a sample properties file for this option, which creates an entry for webgate in Access Manager:

```
WLSHOST: adminvhn.example.com
WLSPORT: 7001
WLSADMIN: weblogic
IDSTORE_HOST: idstore.example.com
IDSTORE_PORT: 389
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=example,dc=com
IDSTORE_SEARCHBASE: dc=example,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=example,dc=com
IDSTORE_OAMSOFTWAREUSER: oamLDAP
IDSTORE_OAMADMINUSER: oamadmin
PRIMARY_OAM_SERVERS: oamhost1.example.com:5575,oamhost2.example.com:5575
WEBGATE_TYPE: ohsWebgate11g
ACCESS_GATE_ID: Webgate_IDM
OAM11G_IDM_DOMAIN_OHS_HOST:sso.example.com
OAM11G_IDM_DOMAIN_OHS_PORT:443
OAM11G_IDM_DOMAIN_OHS_PROTOCOL:https
OAM11G_OAM_SERVER_TRANSFER_MODE:simple
OAM11G_IDM_DOMAIN_LOGOUT_URLS: /console/jsp/common/logout.jsp,/em/targetauth/
emaslogout.jsp
OAM11G_WG_DENY_ON_NOT_PROTECTED: false
OAM11G_SERVER_LOGIN_ATTRIBUTE: uid
OAM_TRANSFER_MODE: simple
COOKIE_DOMAIN: .example.com
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
OAM11G_SSO_ONLY_FLAG: false
OAM11G_OIM_INTEGRATION_REQ: true or false
OAM11G_IMPERSONATION_FLAG:true
OAM11G_SERVER_LBR_HOST:sso.example.com
OAM11G_SERVER_LBR_PORT:443
OAM11G_SERVER_LBR_PROTOCOL:https
COOKIE_EXPIRY_INTERVAL: -1
OAM11G_OIM_OHS_URL:https://sso.example.com:443/
SPLIT_DOMAIN: true
OAM11G_IDSTORE_NAME: OAMIDStore
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=example,dc=com
```

Usage Notes

When you execute this command, the tool prompts you for:

- Password of the identity store account to which you are connecting
- Access Manager administrator password
- Access Manager software user password

In the IBM WebSphere environment:

- Run `idmconfigtool` from the Oracle Access Manager WebSphere cell.
- Provide details of the IBM WebSphere server by specifying the following in the properties file:
  - `WLSHOST` - The WebSphere Application Server host
  - `WLSPORT` - The WebSphere Application Server bootstrap port
  - `WLSADMIN` - Login ID for the Oracle Access Management Console.

> **See Also:**
>
> Table C-2 for details of the properties.

D

Configuring User-Defined Fields

Configure custom attributes or User-Defined Fields (UDFs) for the user, role, organization, and catalog entities.

1. Configure UDFs.

   See Configuring UDFs

   > **Note:**
   >
   > Due to SSO Integration, the following steps must be done for existing SSO users after a Custom UDF is added, to be able to see the Custom UDF.
   >
   > a. Create a Sandbox in the System Administration Console
   >
   > b. Navigate to **Upgrade**, **Upgrade User Form**
   >
   > c. Verify the Custom UDF is listed and then select **Upgrade Now**
   >
   > d. Publish the Sandbox
   >
   > .

2. For role entity, extending schema is not supported for LDAP Synchronization.
3. Add attribute mapping after creating the UDF. See Managing Application OnBoarding.

E

Modifying OIG to Revert OIG-OAM Integration Configuration

1. Revert Weblogic Authentication providers changes in OIG Domain.
   a. Login into Weblogic Administration console for OIG domain.
   b. Navigate to Security Realms>>Providers>>Authentication.
   c. Delete the following authentication providers:
      i. Delete OAMIDAsserter
      ii. Delete OIMSignatureAuthenticator
      iii. Delete OIDAuthenticator, if the directory type used is OID

      > **Note:**
      >
      > If the directory type is OUD or AD, delete OUDAuthenticator or ADAuthenticator respectively.

   d. Create a new authentication provider.
      i. Select New.
      ii. Enter OIMAuthenticationProvider as the name of the new authenticator.
      iii. Select Type as `OIMAuthenticationProvider`.
      iv. Click **OK**.
      v. After creating the authenticator, navigate to OIMAuthenticationProvider details page.
      vi. Set control flag to `SUFFICIENT`.
      vii. Click **Save**.
   e. Reorder Authentication Providers. Select **Reorder** and sort the authenticator providers as follows:
      i. DefaultAuthenticator
      ii. OIMAuthenticationProvider
      iii. TrustService Identity Assert
      iv. DefaultIdentityAsserter
      v. Other authentication providers/asserters, if any.
2. Delete event-handler file from MDS.

   Login into Oracle Enterprise Manager (EM) in OIG Domain to delete metadata files from MDS. See https://docs.oracle.com/middleware/12213/oig/OMDEV/deploying-and-undeploying-customizations.htm#OMDEV5274.

> **Note:**
>
> Use file name as /db/ssointg/EventHandlers.xml and start the process.

3. Disable SSOEnabled flag from SSOIntegrationMXBean.
   a. Login into Oracle Enterprise Manager in OIG Domain.
   b. Select Weblogic Domain >> System MBean Browser.
   c. Navigate to Application Defined Mbeans >> oracle.iam >> Server: oim_server >> Application: oim >> IAMAppRuntimeMBean >> SSOIntegrationMXBean
   d. From the SSOIntegrationMXBean's Attributes tab, set SsoEnabled value to false.
   e. Click **Apply**.
4. Delete the oim.conf from OHS domain.

   If you have copied the oim.conf file manually to OHS domain, then delete $OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf/oim.conf from OHS domain.
5. Restart OHS Server, OIG and OAM domain.

F

Upgrading OIG-OAM Integrated Environments

You can upgrade your existing 11*g* and 12*c* OIG and OAM integrated environments to the latest 12*c* (12.2.1.4.0) release version.

F.1 About the Starting Points for an OIM-OAM Integrated Environment Upgrade

You can upgrade to OIM-OAM Integrated Environment 12c (12.2.1.4.0) from the supported 11*g* or 12*c* releases.

The steps to upgrade OIM-OAM Integrated Environment to 12*c* (12.2.1.4.0) depend on the following existing production topology:

- OIG and OAM 12*c* (12.2.1.3.0) connector-based integrated environment with directories such as Oracle Unified Directory, Oracle Internet Directory, or Active Directory.
- OAM 12*c* (12.2.1.3.0) with latest bundle patches applied and OIG 12*c* (12.2.1.4.0) with bundle patch 12.2.1.4.200505 applied with supported directories like Oracle Unified Directory 12.2.1.3.0 or Oracle Internet Directory 12.2.1.3.0.
- OIG 12*c* (12.2.1.3.0) with latest bundle patches applied and OAM 12*c* (12.2.1.4.0) bundle patch 12.2.1.4.200327 applied with supported directories like such Oracle Unified Directory 12.2.1.3.0 or Oracle Internet Directory 12.2.1.3.0.
- OIG and OAM 11*g* (11.1.2.3.0) LDAP synchronization integrated environment with directories such as Oracle Unified Directory, Oracle Internet Directory, or Active Directory.

> **Note:**
>
> To upgrade to 12.2.1.4.0 from 11.1.2.3.0, you must first upgrade to 12.2.1.3.0, and then upgrade to 12.2.1.4.0.

F.2 Upgrading an OAM-OIM Integrated Environment from a Previous 12c Release

You can upgrade an OAM-OIM integrated environment from a previous 12c release to 12c (12.2.1.4.0).

Complete the steps in the following topics to perform the upgrade:

- Task 1: Upgrading the OAM Environment
- Task 2: Upgrading the OIG Environment

> **Note:**
>
> You can upgrade Oracle Identity and Access Management highly available 12c (12.2.1.3.0) environments to 12c (12.2.1.4.0) using the procedure described in the following topics:
>
> - Upgrading Oracle Access Management Highly Available Environments in the *Upgrading Oracle Identity and Access Management*.
>
> When you install the binaries, you must apply the OAM bundle patch 12.2.1.4.200327 or the latest bundle patch available for your release.
> - Upgrading Oracle Identity Manager Highly Available Environments in the *Upgrading Oracle Identity and Access Management*.
>
> When you install the binaries, you must apply the OIM bundle patch 12.2.1.4.200505 or the latest bundle patch available for your release.

F.2.1 Task 1: Upgrading the OAM Environment

You can upgrade the OAM environment by installing the Oracle Identity and Access Management and Oracle Fusion Middleware Infrastructure 12*c* (12.2.1.4.0) software, applying the latest bundle patch, and copying the required files.

> **Note:**
>
> Before you start upgrading OAM environment, review all introductory information to understand the standard upgrade topologies and upgrade paths for Oracle Identity and Access Management. For more information, see Introduction to Upgrading Oracle Access Manager to 12c (12.2.1.4.0) in *Upgrading Oracle Identity and Access Management*.

Perform the following steps to upgrade the OAM environment.

1. Shut down all of the pre-upgrade processes and servers, including the Administration Server, any Managed Servers, and Node Manager. For more information, see Stopping Servers and Processes in *Upgrading Oracle Identity and Access Management*.
2. Back up and rename the 12.2.1.3.0 OAM Oracle home (`ORACLE_HOME`).

   An Oracle home consists of product homes, such as the WebLogic Server home, an Oracle Common home (Contain the OAM binaries), and the `user_projects` directories (Contains Oracle WebLogic Server domains).

   Example:

   ```
   /u01/app/fmw/ORACLE_HOME_old
   ```
3. Complete the pre-upgrade tasks, as described in Pre-Upgrade Requirements in *Upgrading Oracle Identity and Access Management*.

4. Install the 12c (12.2.1.4.0) OAM binaries in the existing 12c (12.2.1.3.0) OAM Oracle home (`/u01/app/fmw/ORACLE_HOME`) using:
   - Oracle Fusion Middleware Infrastructure (`fmw_12.2.1.4.0_infrastructure.jar`)
   - Oracle Identity and Access Management (`fmw_12.2.1.4.0_idm.jar`)

   For more information about installing the Oracle Access Manager, see Installing Product Distributions in *Upgrading Oracle Identity and Access Management*.

   > **Note:**
   >
   > OAM 12.2.1.4.0 requires Java Development Kit (JDK) 1.8.0_211 and later. You must update the JDK, as described in About Updating the JDK Location After Installing an Oracle Fusion Middleware Product in *Upgrading Oracle Identity and Access Management*.

5. Copy the `user_projects` folder from the backup of 12.2.1.3.0 OAM Oracle home (`/u01/app/fmw/ORACLE_HOME_old/user_projects/`) to the 12.2.1.4.0 OAM Oracle home (`/u01/app/fmw/ORACLE_HOME`).

   > **Note:**
   >
   > Perform the above step, if your existing 12.2.1.3.0 `DOMAIN_HOME` reside within the 12.2.1.3.0 Oracle home directory.

6. Run OPatch to apply the OAM bundle patch 12.2.1.4.200327 or the latest bundle patch available for your release.

   See Applying the Bundle Patch in the *Oracle Access Management Bundle Patch Readme*.

7. Start the Administration Server and the OAM Managed Server, as described in Starting the Servers in *Installing and Configuring Oracle Identity and Access Management*.

F.2.2 Task 2: Upgrading the OIG Environment

You can upgrade the OIG environment by installing the required 12c (12.2.1.4.0) software, applying the bundle patch, and running the Upgrade Assistant to upgrade product schemas and domain component configurations.

> **Note:**
>
> Do the following before you start upgrading OIG environment:
>
> - Review all introductory information to understand the standard upgrade topologies and upgrade paths for Oracle Identity and Access Management. See Introduction to Upgrading Oracle Identity and Access Management to 12c in *Upgrading Oracle Identity and Access Management*.
> - Perform pre-upgrade tasks such as cloning your current environment, verifying that your system meets certified requirements, and so on. See Pre-Upgrade Requirements in *Upgrading Oracle Identity and Access Management*.

Perform the following steps to upgrade the OIG environment.

1. Run the pre-upgrade report utility before you begin the upgrade process for Oracle Identity Manager. For more information about the pre-upgrade report utility, see Generating and Analysing Pre-Upgrade Report for Oracle Identity Manager in *Upgrading Oracle Identity and Access Management*.
2. Complete the tasks described in Completing the Pre-Upgrade Tasks for Oracle Identity Manager in *Upgrading Oracle Identity and Access Management*.
3. Shut down all of the pre-upgrade processes and servers, including the Administration Server, any Managed Servers, and Node Manager.

   See Stopping Servers and Processes in *Upgrading Oracle Identity and Access Management*.
4. Back up and rename the 12.2.1.3.0 OIG Oracle home (`ORACLE_HOME`).

   Example:

   `/u01/app/fmw/ORACLE_HOME_old`
5. Install the 12c (12.2.1.4.0) OIG binaries in the existing 12c (12.2.1.3.0) OIG Oracle home (`/u01/app/fmw/ORACLE_HOME`) using the generic Installer or the quickstart Installer.

   If you are using the generic installer, then obtain the following distributions:

   - Oracle Fusion Middleware Infrastructure (`fmw_12.2.1.4.0_infrastructure.jar`)
   - Oracle SOA Suite (`fmw_12.2.1.4.0_soa_generic.jar`)
   - Oracle Identity and Access Management (`fmw_12.2.1.4.0_idm.jar`)

   If you are using quickstart installer to install all the software in one go, obtain the following distributions:

   - `fmw_12.2.1.4.0_idmquickstart_generic.jar`

   > **Note:**
   >
   > It is recommended that you use the simplified installation process to install the product, using the quickstart installer.

   For more information, see Installing Oracle Identity Governance Using Quickstart Installer in *Installing and Configuring Oracle Identity and Access Management*.
6. Copy the `user_projects` folder from the backup of 12.2.1.3.0 Oracle home (`/u01/app/fmw/ORACLE_HOME_old/user_projects/`) to the 12.2.1.4.0 Oracle home (`/u01/app/fmw/ORACLE_HOME`).

   > **Note:**
   >
   > Perform the above step, if your existing 12.2.1.3.0 `DOMAIN_HOME` reside within the 12.2.1.3.0 Oracle home directory.

7. Run OPatch to apply the OIM bundle patch 12.2.1.4.200505 or the latest bundle patch available for your release, as described in Patching the Oracle Binaries (OPatch Stage) in *Oracle Identity Governance Bundle Patch Readme*.

> **Note:**
>
> Do not start the OIG servers after applying the bundle patch.

8. Update the latest JDK version in the domain home. See Updating the JDK location in *Upgrading Oracle Identity and Access Management*.
9. Run a readiness check before you start the upgrade process. See Running a Pre-Upgrade Readiness Check in *Upgrading Oracle Identity and Access Management*.
10. Tune the Database parameters for Oracle Identity Manager. See Tuning Database Parameters for Oracle Identity Manager in *Upgrading Oracle Identity and Access Management*.
11. Run the Upgrade Assistant from the 12c (12.2.1.4.0) Oracle home to upgrade product schemas, as described in Upgrading Product Schemas in *Upgrading Oracle Identity and Access Management*.

> **Note:**
>
> Ensure that you select **All Schemas Used by a Domain** in the **Selected Schemas** screen.

12. Run the Upgrade Assistant from the 12c (12.2.1.4.0) Oracle home to upgrade domain component configurations, as described in Upgrading Domain Component Configurations in *Upgrading Oracle Identity and Access Management*.
13. Start the WebLogic Admin Server, SOA Managed Servers, and Oracle Identity Governance Managed Server. For more information about starting the servers, see Starting the Servers in *Installing and Configuring Oracle Identity and Access Management*.

> **Note:**
>
> When you start the Oracle Identity Governance server, the bootstrap report is generated at `DOMAIN_HOME/servers/oim_server1/logs/BootStrapReportPreStart.html`. For more information about the bootstrap report, see Analyzing the Bootstrap Report in *Installing and Configuring Oracle Identity and Access Management*.

14. Open the `patch_oim_wls.profile` file (Located in the `ORACLE_HOME/idm/server/bin/` directory) in a text editor, and change the values in the file to match your environment.

    See Filling in the patch_oim_wls.profile File in *Oracle Identity Governance Bundle Patch Readme*.
15. Patch the OIG Managed Servers on WebLogic by performing the following steps:
    a. Set the following environment variables:

UNIX

```
setenv PATH $JAVA_HOME/bin:$PATH
```

Windows

```
set JAVA_HOME=VALUE_OF_JAVA_HOME
set ANT_HOME=\PATH_TO_ANT_DIRECTORY\ant
set ORACLE_HOME=%MW_HOME%\idm
```

> **Note:**
>
> Make sure to set the reference to JDK binaries in your PATH before running the `patch_oim_wls.sh` (UNIX) or `patch_oim_wls.bat` (Microsoft Windows) script. This `JAVA_HOME` must be of the same version that is being used to run the WebLogic servers. The `JAVA_HOME` version from `/usr/bin/` or the default is usually old and must be avoided. You can verify the version by running the following command:

b. Execute `patch_oim_wls.sh` (UNIX) or `patch_oim_wls.bat` (Microsoft Windows) to apply the configuration changes to the Oracle Identity Governance server.

c. Delete the following directory in domain home:

`DOMAIN_HOME//servers/oim_server1/tmp/_WL_user/oracle.iam.console.identity.self-service.ear_V2.0`
Here, `oim_server1` is the weblogic manged server used for OIG.

d. To verify that the `patch_oim_wls` script has completed successfully, check the `ORACLE_HOME/idm/server/bin/patch_oim_wls.log` log file.

16. Restart the Administration Server, Oracle SOA Suite Managed Server, and the OIG Managed Server. See Starting the Servers in the *Upgrading Oracle Identity and Access Management*.

> **Note:**
>
> Depending on your OIG environment, you may need to perform additional post-upgrade task. See Post-Upgrade Task in *Upgrading Oracle Identity and Access Management*.

F.3 Upgrading an OAM-OIM Integrated Environment from a 11*g* Release

You can upgrade your OAM-OIG LDAP synchronization integrated environment 11*g* Release 2 (11.1.2.3.0) version to the latest 12*c* (12.2.1.4.0) release version. To upgrade to 12*c* (12.2.1.4.0), you must first upgrade to 12*c* (12.2.1.3.0), and then upgrade to 12*c* (12.2.1.4.0).

> **Note:**
>
> If you upgrade from 11*g* Release 2 (11.1.2.3.0) version to the latest 12*c* (12.2.1.4.0), then you must disable the LDAP synchronization integrated environment and migrate to LDAP connector-based integrated environment.

Complete the steps in the following topics to perform the upgrade:

- Task 1: Upgrading the Integrated Environments
- Task 2: Configuring Oracle HTTP Server
- Task 3: Prerequisites for the Connector-based Integration
- Task 4: Disabling LDAP Synchronization
- Task 5: Configuring WLS Authentication Providers
- Task 6: Configuring the LDAP Connector
- Task 7: Configuring SSO Integration
- Task 8: Enabling OAM Notifications
- Task 9: Adding Missing Object Classes
- Task 10: Restarting Servers
- Task 11: Performing Post-Upgrade Task
- Task 12: Validating the Integrated Environments

F.3.1 Task 1: Upgrading the Integrated Environments

To upgrade your 11*g* Release 2 (11.1.2.3.0) environment, complete the following steps:

1. Upgrade your existing 11*g* Release 2 (11.1.2.3.0) integrated environment to Oracle Identity and Access Management 12*c* (12.2.1.3.0).

   See:

   - Introduction to Upgrading Oracle Access Manager to 12c (12.2.1.3.0) in in *Upgrading Oracle Access Manager*.
   - Introduction to Upgrading Oracle Identity Manager to 12c (12.2.1.3.0) in *Upgrading Oracle Identity Manager*.

2. After upgrading the integrated environment to OAM-OIM 12c (12.2.1.3.0), perform the following:

   a. If you have an existing Oracle Internet Directory 11*g* connector or Microsoft Active Directory User Management (AD User Management) 11*g* connector deployed for provisioning and reconciliation then you can use the same connectors for Single sign-on (SSO). To do so, you must upgrade the connectors to 12.2.1.3.0.

      For more information about the upgrade, see the following:

      - Upgrading the Oracle Internet Directory Connector in the *Configuring the Oracle Internet Directory Application*.
      - Upgrading the Microsoft Active Directory User Management Connector in the *Configuring the Microsoft Active Directory User Management Application*.

b. If any self-registration request is in pending state, then you must approve all pending requests using the Oracle Identity Self Service Interface.

   See Managing Pending Approvals in the *Performing Self Service Tasks with Oracle Identity Governance*.

3. Upgrade the OAM-OIM 12c (12.2.1.3.0) integrated environment that you have upgraded from 11*g* Release 2 (11.1.2.3.0) to 12c (12.2.1.4.0), as described in Upgrading an OAM-OIM Integrated Environment from a Previous 12c Release.

F.3.2 Task 2: Configuring Oracle HTTP Server

You can configuring the Oracle HTTP Server to front-end resources on OIG.

> **Note:**
>
> You can upgrade your earlier version of Oracle HTTP Server to the 12*c* (12.2.1.4.0) release. For more information about upgrade, see Introduction to Upgrading Oracle HTTP Server to 12c (12.2.1.4.0) *Upgrading Oracle HTTP Server*.

Configure the Oracle HTTP Server for the integrated environment, by completing the following steps:

1. Configure the Oracle HTTP Server WebGate for Oracle Access Management, as described in the section Installing Oracle HTTP Server and Configuring the Oracle HTTP Server WebGate
2. Populating the Oracle HTTP Server rules, as described in the section Populating OHS Rules Using Automated Script
3. If you have upgraded your 11*g* release or previous 12*c* release to the 12*c* (12.2.1.4.0) release then do the following:
   a. Open a text editor and compare the older `oim.conf` file from your previous release with the new `oim.conf` file that you generated by running the `OIGOAMIntegration.sh` script.
   b. Add any missing parameters from the older `oim.conf` file to the new `oim.conf` file.
   c. Save the file when done.
   d. Restart OHS Server.

F.3.3 Task 3: Prerequisites for the Connector-based Integration

Before you begin to migrate from a LDAP synchronization integrated environment to a connector-based integrated environment, you must complete the prerequisites such as setting the environment variables, updating the datasource, and downloading the connector bundle.

Complete the following prerequisites in this section before migrating from a LDAP synchronization integrated environment to a connector-based integrated environment.

1. Back up all system-critical files, including the databases that host your Oracle Fusion Middleware 12.2.1.4.0 schemas. For more information, see Creating a Complete Backup in *Upgrading Oracle Identity and Access Management*.

   > **Note:**
   >
   > If any step in the migration from a LDAP synchronization integrated environment to a connector-based integrated environment process fails, restore the environment to its original state using the backup files you created.

2. Before running the `OIGOAMIntegration.sh` script to enable connector-based integrated environment, do the following:

   a. Set the environment variables to the full path of the 12.2.1.4.0 OIG Oracle home, as shown in the following example:

   ```
   export ORACLE_HOME=/u01/Oracle_Home
   export MW_HOME=/u01/Oracle_Home
   export OIM_ORACLE_HOME=/u01/Oracle_Home/idm/
   export WL_HOME=/u01/Oracle_Home/wlserver
   export JAVA_HOME=<<Java Home location>>
   ```

   b. On UNIX, provide the executable permission for the `OIGOAMIntegration.sh` script in the 12.2.1.4.0 OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/bin`):

   ```
   chmod 777 _OIGOAMIntegration.sh
   chmod 777 OIGOAMIntegration.sh
   ```

3. Complete the prerequisites described in the section Prerequisites for the Connector-based Integration.

4. If you have upgraded the Oracle Internet Directory 11*g* connector or Microsoft Active Directory User Management 11g connector to 12.2.1.3.0, as describe in Step 2.a, then you must complete the following steps:

   a. Navigate to the directory (For example, OID/OUD the folder is named `OID-12.2.1.3.0` and AD the folder is named `activedirectory-12.2.1.3.0`) that has the connector that you upgraded from 11g to 12.2.1.3.0, and then copy one of the following folders depending on the LDAP directory to the backup of 12.2.1.3.0 OIG home directory.

   - OID/OUD: `OID-12.2.1.3.0`
   - AD: `activedirectory-12.2.1.3.0`

   Example:

   OID/OUD: `ORACLE_HOME_old/idm/server/ConnectorDefaultDirectory/OID-12.2.1.3.0`

   AD: `ORACLE_HOME_old/idm/server/ConnectorDefaultDirectory/activedirectory-12.2.1.3.0`

   b. Navigate to the directory (For example, OID/OUD the folder is named `OID-12.2.1.3.0` and AD the folder is named `activedirectory-12.2.1.3.0`), and then copy one of the following folders depending on you LDAP directory to the 12.2.1.4.0 OIG home directory.

- OID/OUD: `OID-12.2.1.3.0`
- AD: `activedirectory-12.2.1.3.0`

Example:

OID/OUD: `ORACLE_HOME/idm/server/ConnectorDefaultDirectory/OID-12.2.1.3.0`

AD: `ORACLE_HOME/idm/server/ConnectorDefaultDirectory/activedirectory-12.2.1.3.0`

c. Open the `configureLDAPConnector.config` file from the 12.2.1.4.0 OIG Oracle home directory in a text editor and update the `CONNECTOR_MEDIA_PATH` parameter with the full path of the 12.2.1.3.0 backup OIG folder as shown in the following example:

- OID/OUD: `CONNECTOR_MEDIA_PATH=/u01/app/fmw/ORACLE_HOME/idm/server/ConnectorDefaultDirectory/OID-12.2.1.3.0`
- AD: `CONNECTOR_MEDIA_PATH=/u01/app/fmw/ORACLE_HOME/idm/server/ConnectorDefaultDirectory/activedirectory -12.2.1.3.0`

F.3.4 Task 4: Disabling LDAP Synchronization

This section describes how to disable the LDAP synchronization.

Complete the following steps:

1. Open the `migrateOIMOAMIntegration.config` file from the 12.2.1.4.0 OIG Oracle home directory (Located at `ORACLE_HOME/idm/server/ssointg/config`) in a text editor and update the parameters.

Example `migrateOIMOAMIntegration.config` File

```
IDSTORE_DIRECTORYTYPE
OIM_WLSHOST
OIM_WLSPORT
OIM_WLSADMIN
OIM_WLSADMIN_PWD
OIM_SERVER_NAME
OIM_HOST
OIM_PORT
WLS_OIM_SYSADMIN_USER
WLS_OIM_SYSADMIN_USER_PWD
MDS_EXPORT_PATH
```

The following table describes the parameters that you can set in the `migrateOIMOAMIntegration.config` file.

Table F-1 Parameters in migrateOIMOAMIntegration.config File

Parameters	Description	Sample Value
`IDSTORE_DIRECTORYTYPE`	Enter the identity store directory type. Valid options are OID, OUD, and AD.	`OUD`

Table F-1 (Cont.) Parameters in migrateOIMOAMIntegration.config File

Parameters	Description	Sample Value
OIM_WLSHOST	Enter the OIG admin server host name.	oimadminhost.example.com
OIM_WLSPORT	Enter the OIG admin server port.	17001
OIM_WLSADMIN	Enter the weblogic administrator user in OIM domain.	weblogic
OIM_WLSADMIN_PWD	Enter the password for the weblogic admin user in OIM domain.	*password*
OIM_SERVER_NAME	Enter the OIG server name.	oim_server1
OIM_HOST	Enter the host name for OIG managed server.	oimhost.example.com
OIM_PORT	Enter the port for OIG Server.	14000
WLS_OIM_SYSADMIN_USER	Enter the system admin user to be used to connect to OIG while configuring SSO. This user needs to have system admin role.	xelsysadm
WLS_OIM_SYSADMIN_USER_PWD	Enter the password for OIG system administrator user.	*Password*
MDS_EXPORT_PATH	Specify location to export MDS.	/u01/app/upgrade/backup

2. Run the `OIGOAMIntegration.sh` script from the 12.2.1.4.0 `ORACLE_HOME` (Located at `ORACLE_HOME/idm/server/ssointg/bin`) to delete the `EventHandlers.xml` file from MDS and disable all LDAP scheduled jobs:

   ```
   ./OIGOAMIntegration.sh -migrateOIMOAMIntegration
   ```

3. Delete the adapters configured for the libOVD configuration:

   a. Invoke WLST interactively by running the following command from the 12.2.1.4.0 OIG Oracle home directory:

      ```
      ORACLE_HOME/oracle_common/common/bin/wlst.sh
      ```

   b. Connect to the WebLogic Administration Server:

      ```
      connect('Weblogic_User', 'Weblogic_password', 't3://
      Weblogic_Host:Weblogic_AdminServer_Port')
      ```
      Example:

      ```
      connect('weblogic', 'Password', 't3://example.com:7001')
      ```

   c. Lists the name and type of all adapters that are configured.

      ```
      listAdapters([contextName])
      ```

Example:

```
listAdapters(contextName='oim')
```

See listAdapters in the *WebLogic Scripting Tool Command Reference for Identity and Access Management*.

d. Deletes all the existing adapter for the libOVD configuration:

```
deleteAdapter(adapterName, [contextName])
```

Example:

```
deleteAdapter(adapterName='oud1', contextName='oim')
deleteAdapter(adapterName='CHANGELOG_oud1', contextName='oim')
```

See deleteAdapter in *WebLogic Scripting Tool Command Reference for Identity and Access Management*.

F.3.5 Task 5: Configuring WLS Authentication Providers

You must configure the WLS Authentication Providers to set SSO logout for and security providers in OIG domain. So that both the SSO login and OIM client-based login, work appropriately.

Configure the WLS Authentication Providers by performing the steps described in the section Configuring WLS Authentication Providers Using Automated Script.

F.3.6 Task 6: Configuring the LDAP Connector

Configure LDAP Connector by performing the steps described in the section Configuring LDAP Connector Using Automated Script.

F.3.7 Task 7: Configuring SSO Integration

You must configure SSO integration to register OIM as TAP partner for OAM, add the resource policies for OIG-OAM communication, and update `SSOIntegrationMXBean` values in MDS.

To configure SSO integration, perform the steps described in the section Configuring SSO Integration Using Automated Script.

F.3.8 Task 8: Enabling OAM Notifications

Enable the OAM notification handlers and register OIG System Administrator to utilize OAM REST APIs.

To enable OAM notification, complete the steps described in the section Enabling OAM Notifications Using Automated Script.

F.3.9 Task 9: Adding Missing Object Classes

Add missing object classes for existing users in LDAP directory (Oracle Internet Directory or Oracle Unified Directory) using the `OIGOAMIntegration.sh` automated script.

> **Note:**
>
> This feature is not available for the Active Directory.

To add the missing object classes, complete the steps described in the section Adding Missing Object Classes Using Automated Script.

F.3.10 Task 10: Restarting Servers

Restart all processes and servers, including the Administration Server and any Managed Servers for OAM and OIG.

To start your servers:

1. Restart OHS Server. For information about starting the server, see Restarting Oracle HTTP Server Instances in *Administering Oracle HTTP Server*.
2. To start Node Manager, use the `startNodeManager` script:

   UNIX

   ```
   DOMAIN_HOME/bin/startNodeManager.sh
   ```

   Windows

   ```
   DOMAIN_HOME\bin\startNodeManager.cmd
   ```

3. To start the Administration Server, use the `startWebLogic` script:

   UNIX

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

   Windows

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

   When prompted, enter your user name, password, and the URL of the Administration Server.
4. To start a WebLogic Server Managed Server, use the `startManagedWebLogic` script:

   UNIX

   ```
   DOMAIN_HOME/bin/startManagedWebLogic.sh managed_server_name admin_url
   ```

Windows

```
DOMAIN_HOME\bin\startManagedWebLogic.cmd managed_server_name
admin_url
```

When prompted, enter your user name, password, and the URL of the Administration Server.

> **Note:**
>
> For SOA and OIG Managed Servers, specify the URL of the Administration Server in the OIG domain.

F.3.11 Task 11: Performing Post-Upgrade Task

After you complete the upgrade and migrate to connector-based integrated environment, perform the following steps:

1. Open a browser, and access the Oracle Identity System Administration Console using the following URL format:

   `http://HOSTNAME:PORT/sysadmin`

   In this `URL`, `HOSTNAME` represents the name of the computer hosting the Oracle HTTP Server and `PORT` refers to the port on which the Oracle HTTP Server is listening.
2. In the left panel, under **System Configuration** , click **Configuration Properties**.
3. Enter `SSOIntegration.GroupRecon.OIGRole.Matching.RoleName` in the Search field.

   > **Note:**
   >
   > If the `SSOIntegration.GroupRecon.OIGRole.Matching.RoleName` property is not available, then you must create it. See Creating System Properties in the *Administering Oracle Identity Governance*.

4. Click the icon next to the Search field. The `SSOIntegration.GroupRecon.OIGRole.Matching.RoleName` system property is displayed.
5. In the Property Name column of the search results table, click the `SSOIntegration.GroupRecon.OIGRole.Matching.RoleName` system property. The System Property Details page is displayed.
6. Set the value to `true` and click **Save** to save the changes made.
7. Run the **SSO Group Create And Update Full Reconciliation** job to import the new roles from target and update the existing roles in OIG:
   a. In the left panel, under **System Configuration** , click **Scheduler**.
   b. On the left pane, in the search results table, click `SSO Group Create And Update Full Reconciliation` then from the Actions list, click **Run Now**.

8. Run the **Roles Migration on Post LDAP Sync to SSO Integration** job to auto seed the necessary artifacts for the existing roles in OIG:
   a. In the left panel, under **System Configuration** , click **Scheduler**.
   b. On the left pane, in the search results table, click `Roles Migration on Post LDAP Sync to SSO Integration` then from the Actions list, click **Run Now** .
9. Navigate to **Configuration Properties** under **System Configuration** , click **Configuration Properties** and set the value to `false` for the `SSOIntegration.GroupRecon.OIGRole.Matching.RoleName` system property.
10. Navigate to **Scheduler** under **System Configuration** and run the following reconciliation jobs:
    - SSO User Full Reconciliation
    - SSO Group Membership Full Reconciliation
    - SSO Group Hierarchy Sync Full Reconciliation

F.3.12 Task 12: Validating the Integrated Environments

After the upgrade, you can validate the integrated environments by performing the tasks described in the section Validating the Access Manager and Oracle Identity Governance Integration.

For any common problems you might encounter, see the section Troubleshooting Common Problems in Access Manager and OIG Integration.

For known issue and limitations, see Known Limitations and Workarounds in OIG-OAM Integration.