ORACLE
FUSION MIDDLEWARE

An Oracle White Paper
Feb 2014

# Integrate Oracle E-Business Suite Using Oracle E-Business Suite AccessGate with Oracle Access Manager Using Multiple Data Stores

ORACLE

# Table of Contents

# 1 Introduction

Oracle Access Manager 11g Release 2 (11.1.2.x) provides a comprehensive identity management and access control system that simplifies user access across applications. For more information about Oracle Access Manager, refer to the Oracle Access Manager home page on the Oracle Corporation Web site: http://www.oracle.com/us/products/middleware/identity-management/oracle-access-manager/overview/index.html

For more information on how to integrate Oracle E-Business Suite with Oracle Access Manager refer to the following My Oracle Support Knowledge Document: *Overview of Single Sign-On Integration Options for Oracle E-Business Suite* (Note 1388152.1)

Oracle E-Business Suite requires Oracle Internet Directory be defined as its data store in Oracle Access Manager. Given an organization's policy for user authentication, a different data store may be required for other applications in the environment. Refer to the following blog article to understand more about Oracle E-Business Suite dependencies on Oracle Internet Directory: Why does Oracle E-Business Suite Integration with Oracle Access Manager Require Oracle Internet Directory.

Oracle Access Manager can be used to protect multiple applications and can also be configured to leverage multiple data stores. These features allow for the mandatory requirement of using Oracle Internet Directory as the data store for Oracle E-Business Suite and additional data stores for other applications.

In this document we will discuss approaches organizations can follow to synchronize the user data between Oracle Internet Directory (particularly the orclguid attribute) and the other configured data store in Oracle Access Manager (e.g. Oracle Directory Server Enterprise Edition or other third-party directory services) such that Single Sign-On can happen seamlessly between the protected applications.

- Approach 1 – Using Oracle Virtual Directory
- Approach 2 – Using Oracle Directory Integration Platform

## 1.1 Assumptions

- An existing Oracle E-Business Suite and Oracle Access Manager 11g integrated environment is configured and running. Oracle E-Business Suite will be configured to use Oracle Internet Directory. Please refer to one of the following My Oracle Support Knowledge documents for required steps for the integration:
  - *Overview of Single Sign-On Integration Options for Oracle E-Business Suite* (Note 1388152.1)

- The user has knowledge of the Oracle Access Manager administration console and concepts.

# 2 Proposed Approaches

Note: For the proposed approaches we have used Oracle Directory Server Enterprise Edition as an illustration. This however can be any supported third-party Directory Service.

## 2.1 Approach 1 – Using Oracle Virtual Directory

Oracle Virtual Directory is LDAP v3 enabled service that provides virtualized abstraction of one or more enterprise data sources into a single directory view. It provides the ability to integrate LDAP-aware applications into diverse directory environments while minimizing or eliminating the need to change either the infrastructure or the applications. For additional product information refer to the Oracle Virtual Directory home page: http://www.oracle.com/technetwork/middleware/id-mgmt/index-093158.html

Using this approach Oracle E-Business Suite and other Oracle Access Manager protected applications are configured to use Oracle Virtual Directory as the data store for authentication in Oracle Access Manager

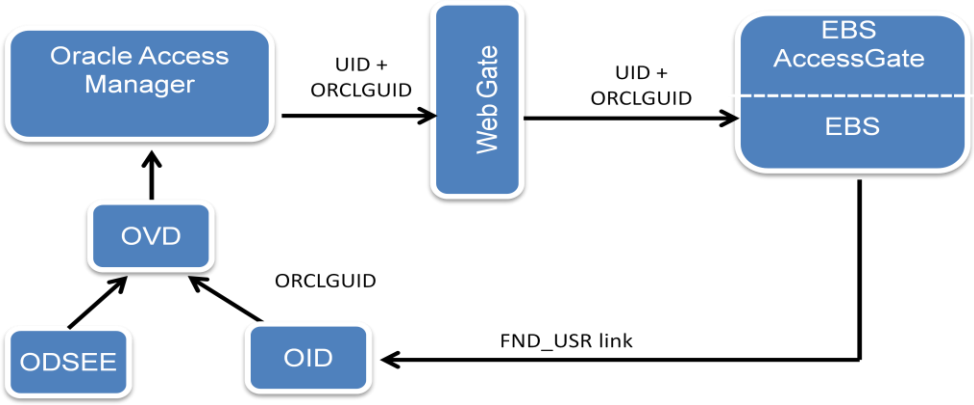


Figure 1. Integration Approach Using Oracle Virtual Directory

At a high level, the following configuration changes need to be done to use this setup:

- Install and Configure Oracle Virtual Directory. Refer to the Oracle Virtual Directory product documentation for the required steps.
- Configure Oracle Virtual Directory Adapters to connect to Oracle Internet Directory and Oracle Directory Server Enterprise Edition LDAP repository – Refer product documentation for the steps

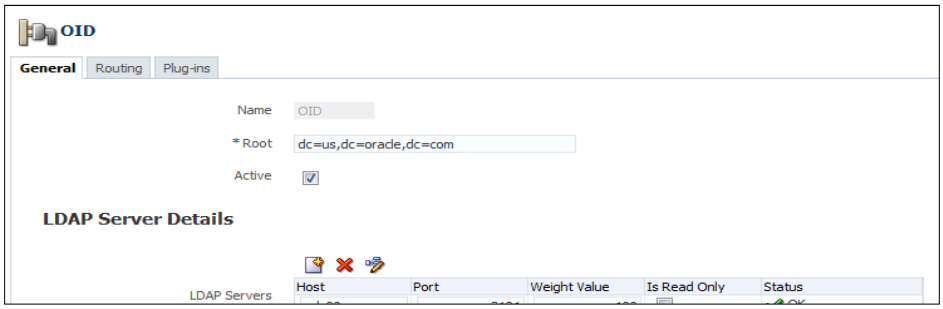


Figure 2.Screenshot of configuring Oracle Internet Directory Adapter in Oracle Virtual Directory

- Configure Oracle Virtual Directory Join Adapter – This combines multiple different data sources into one unified LDAP view similar to a relational database's table join. In this case we are combining Oracle Internet Directory with Oracle Directory Server Enterprise Edition. Refer product documentation for the steps

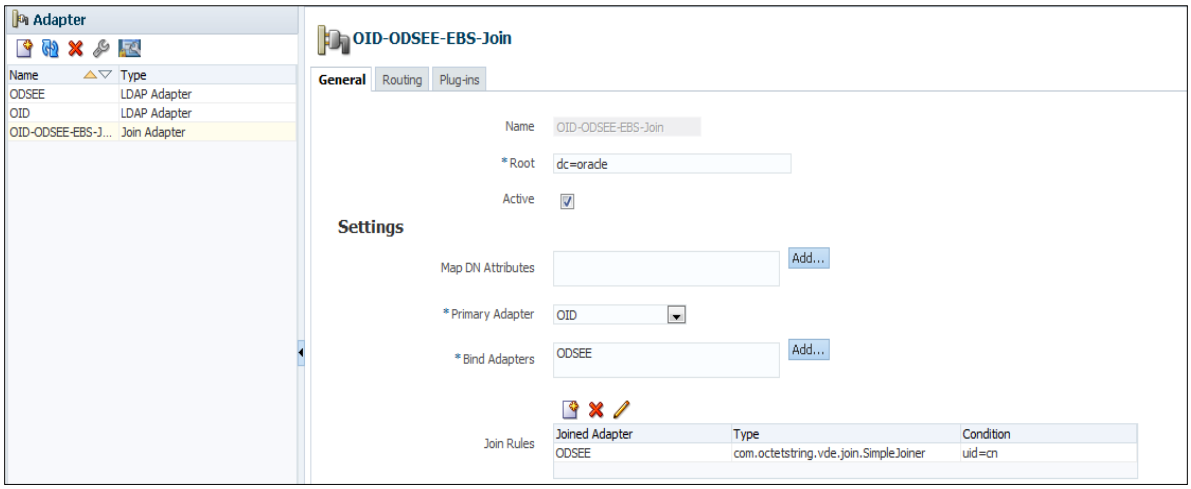


Figure 3.Screenshot of configuring Oracle Virtual Directory Join Adapter

- Create a new User Identity Data store in Oracle Access Manager and configure it to point the Oracle Virtual Directory.
  Refer to product documentation for the steps.

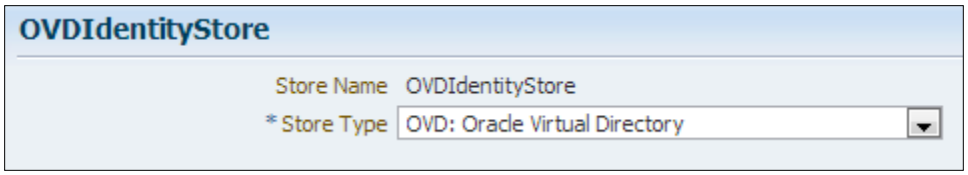


Figure 4.Screenshot of creating a new Identity Data Store in Oracle Access Manager

- Configure authentication module in Oracle Access Manager to leverage Oracle Virtual Directory identity store. Configure an authentication scheme that uses this authentication module. (Note : You can modify existing authentication module/scheme to leverage Oracle Virtual Directory identity store)

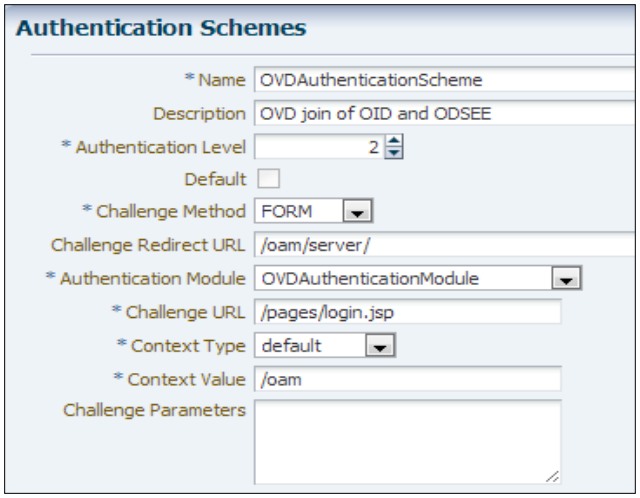


Figure 5.Screenshot of configuring an Authentication Module in Oracle Access Manager

- Configure the authentication policy for each of the protecting applications in the respective application domains to use the new Oracle Virtual Directory authentication scheme

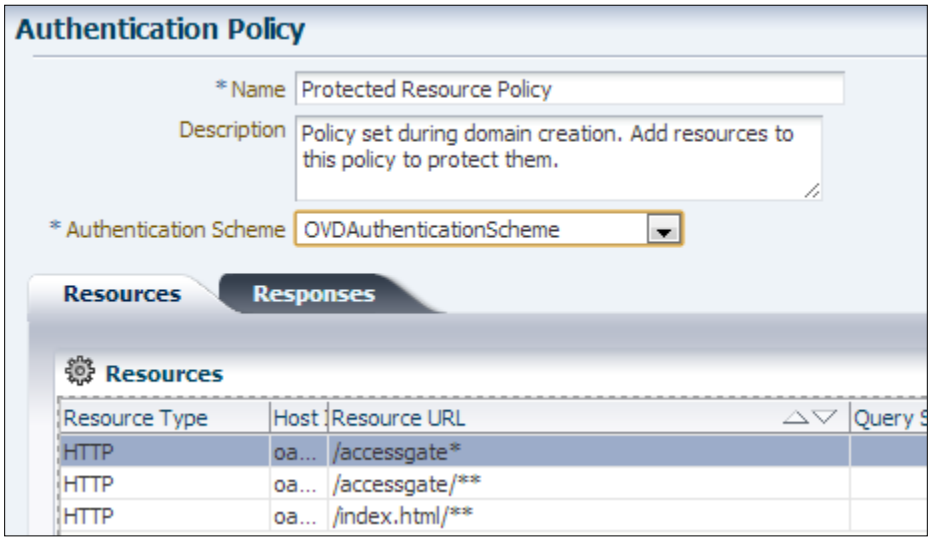


Figure 6.Screenshot of configuring Authentication Policy in Oracle Access Manager

- Once all of the previously described steps are completed, Single Sign-On will work for Oracle E-Business Suite and other protected applications.

## 2.2 Approach 2 – Using Oracle Directory Integration Platform

The Oracle Directory Integration Platform (DIP) enables you to synchronize Oracle Internet Directory data with other data sources. You save time and resources by using Oracle Internet Directory as the central repository for different LDAP-enabled applications and connected directories. Synchronization can be one-way or two-way.

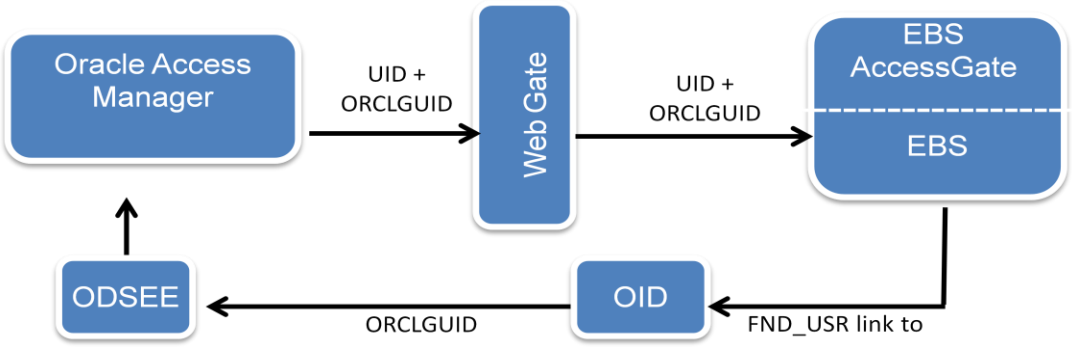


Figure 7.Integration Approach using Oracle Directory Integration Platform

**Requirements for using this approach**

- The user object class in Oracle Directory Server Enterprise Edition needs to be extended to add ORCLGUID attribute.
- New user creation in Oracle Directory Server Enterprise Edition needs to happen via Oracle Internet Directory only (applicable only for users whose entry needs to be present in both Oracle Internet Directory and Oracle Directory Server Enterprise Edition). Whenever a user is created in Oracle Internet Directory a corresponding user entry will be created in Oracle Directory Server Enterprise Edition using the synchronization process
- If a user already exists in Oracle Directory Server Enterprise Edition, and is later on created in Oracle Internet Directory, the corresponding user ORCLGUID value from Oracle Internet Directory will not be reflected in Oracle Directory Server Enterprise Edition
- Initial sync of ORCLGUID attribute for Oracle Directory Server Enterprise Edition users from Oracle Internet Directory needs to be done via DIP bootstrap process. Refer to the DIP product documentation for required steps.
- For users entries that need to be in Oracle Directory Server Enterprise Edition only, existing provisioning process can continue

At a high level, the following configuration changes need to be done to use this setup:

- Install and configure DIP – Refer to the DIP product documentation for required steps.
- A new synchronization profile needs to be created using DIP, that propagates user information from Oracle Internet Directory to Oracle Directory Server Enterprise Edition. Refer to DIP product documentation for the required steps.

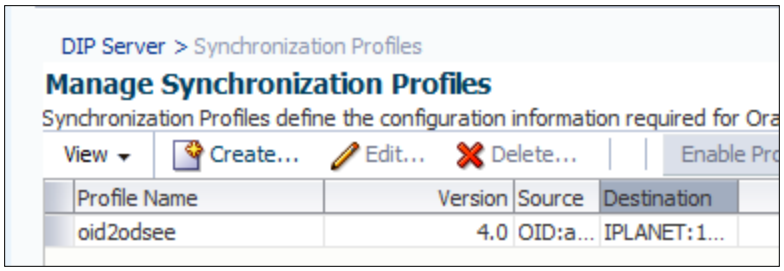


Figure 8.Screenshot of synchronization profile in DIP

- The synchronization profile needs to be created with source as Oracle Internet Directory and target as Oracle Directory Server Enterprise Edition.

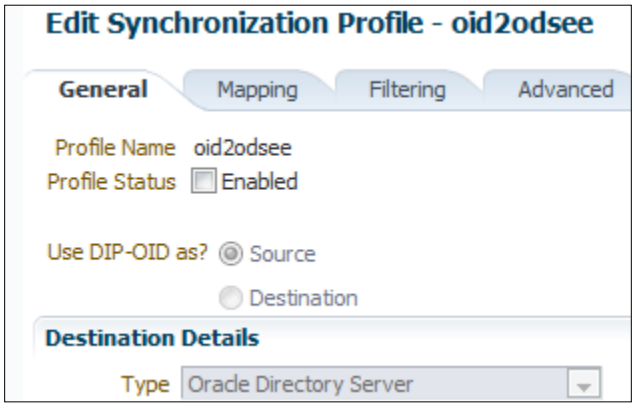


Figure 9.Screenshot of configuring synchronization profile in DIP

- In the Mapping tab for Attribute Mapping Rules make sure to map orclguid attribute from Oracle Internet Directory person schema to corresponding orclguid attribute in the corporate user object class in Oracle Directory Server Enterprise Edition

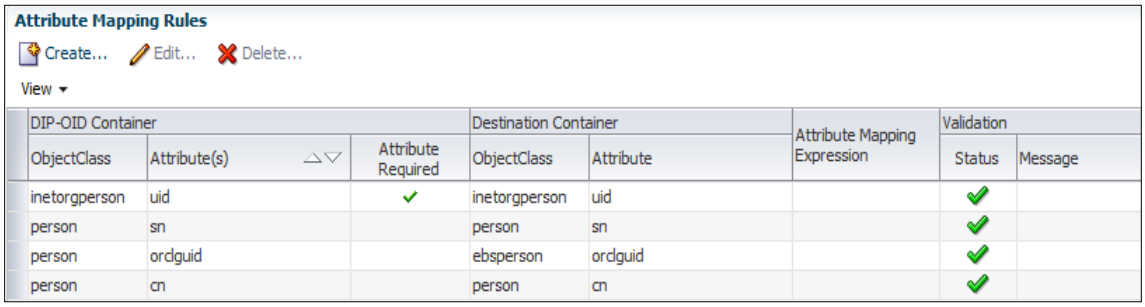


Figure 10.Screenshot of attribute mapping using DIP

- Enable the synchronization profile and schedule it appropriately based on the frequency of user add operation in Oracle Internet Directory.
- There are no changes in Oracle Access Manager configuration for Oracle E-Business Suite and other protected corporate applications. Oracle Directory Server Enterprise Edition remains the primary data store for user identity for all applications in Oracle Access Manager. Oracle E-Business Suite is configured to leverage Oracle Internet Directory

# 3 Which Approach Should You Target

Both approaches described in this white paper are certified configurations. This section discuses some considerations for choosing between Approach 1 – Using Oracle Virtual Directory and Approach 2 – Using Oracle Directory Integration Platform.

Consider targeting Approach 1 – Using Oracle Virtual Directory if the following apply to your organization:

- You are willing to invest in the skills and architecture required to deploy Oracle Virtual Directory or if you already have Oracle Virtual Directory deployed in your organization
- You cannot make changes to your current provisioning process
- You require real-time data synchronization
- You require the flexibility to add new attributes with no schema changes

Consider targeting Approach 2 – Using Oracle Directory Integration Platform if the following apply to your organization:

- You have Oracle Directory Integration Platform experience or are willing to invest in acquiring these skills
- You understand and are willing to make any necessary changes to the provisioning process to support this approach
- Your environment will support data synchronization that is not real time
- You are willing to make schema changes as required to support new attributes that may be added in the future

# 4 References

- Oracle Access Manager
  - Home Page
    http://www.oracle.com/us/products/middleware/identity-management/oracle-access-manager/overview/index.html
- Oracle Virtual Directory
  - Home Page
    http://www.oracle.com/technetwork/middleware/id-mgmt/index-093158.html
  - Product Documentation:
    http://docs.oracle.com/cd/E29542_01/install.1111/e12002/ovd.htm
- Directory Integration Platform
  - Production Documentation
    http://docs.oracle.com/cd/E28280_01/install.1111/e12002/dip.htm
- My Oracle Support Knowledge Documents
  - *Overview of Single Sign-On Integration Options for Oracle E-Business Suite* (Note 1388152.1)
  - Oracle E-Business Technology Blog
    Why does Oracle E-Business Suite Integration with Oracle Access Manager Require Oracle Internet Directory

White Paper Integrate Oracle E-Business Suite Using Oracle E-Business Suite AccessGate with Oracle Access Manager Using Multiple Data Stores
Feb 2014
Author: Sairam Pappu
Contributing Authors: Elke Phelps, Hubert Ferst

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment



**Hardware and Software, Engineered to Work Together**