Oracle® E-Business Suite Concepts

Authentication and Integration

Introduction

The subject of authentication is a broad one, which covers a variety of technologies and components. This chapter provides a survey of the key architectural concepts and decisions involved in setting up the required level of authentication for an organization.

Additional Information: For additional authentication and authorization documentation, refer to My Oracle Support Knowledge Document 1934915.1, *Oracle E-Business Suite Release 12.2 Technology Stack Documentation Roadmap*. In particular, see Document 2003483.1, *Integrating Oracle E-Business Suite Release 12.2 with Oracle Unified Directory 11g Release 2*.

Integrating Oracle E-Business Suite Release 12.2 with Oracle Unified Directory 11g Release 2

Authentication of Oracle E-Business Suite users can be configured to be straightforward and out of the box, using the traditional FND_USER mechanism, or it can involve various additional features and levels of sophistication, such as single sign-on and use of optional products such as Oracle Discoverer.

Additional Information: If applicable, refer to My Oracle Support Knowledge Document 2277369.1, *Oracle E-Business Suite Support Implications for Discoverer 11gR1* .

The system administrator can choose the optimal solution for an installation, taking into account factors such as simplicity of setup and maintenance, the possible need for a single point of access to enterprise-wide applications, and the ability to integrate with third-party user directories, as well as the overall security requirements of the organization.

Note: *Oracle Directory Services* refers to both *Oracle Internet Directory* and *Oracle Unified Directory*. Procedures documented for implementing Oracle Directory Services apply to both these directories.

Advanced features that are discussed briefly include the tasks involved in keeping user profile information automatically synchronized across an enterprise, and the steps needed to link an account in Oracle Directory Services to multiple application accounts in Oracle E-Business Suite Release 12.2.

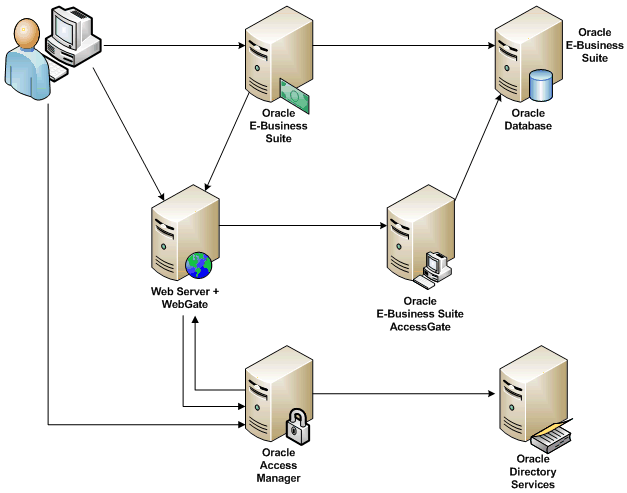
Important: Use of the advanced authentication features described in this chapter, such as Single Sign-On, are optional with Oracle E-Business Suite Release 12.2. If you wish to use them, you must carry out the requisite additional setup procedures as noted later.

The solutions described here do not address the issue of *authorization*. After a user has been authenticated, Oracle E-Business Suite retrieves the authorization information associated with the application account the user is logged into. Authorization information for application accounts is managed through application responsibilities. Oracle E-Business Suite applies authorization checks as and when required during the user's session.

Single Sign-On

Single sign-on functionality enables users to access Oracle E-Business Suite and other applications through a single user ID, without having to log in to each application separately. Oracle E-Business Suite supports the use of single sign-on functionality via two classes of component, each of which performs a distinct but related function. The first class is an LDAP directory such as *Oracle Unified Directory (OUD)*. The second class is a single sign-on product such as *Oracle Access Manager*, which is used in conjunction with *Oracle E-Business Suite AccessGate*, a Java Enterprise Edition application that maps a single sign-on user to an Oracle E-Business Suite user, and creates the Oracle E-Business Suite session for that user.

The following diagram illustrates the high-level structure of a typical integration.

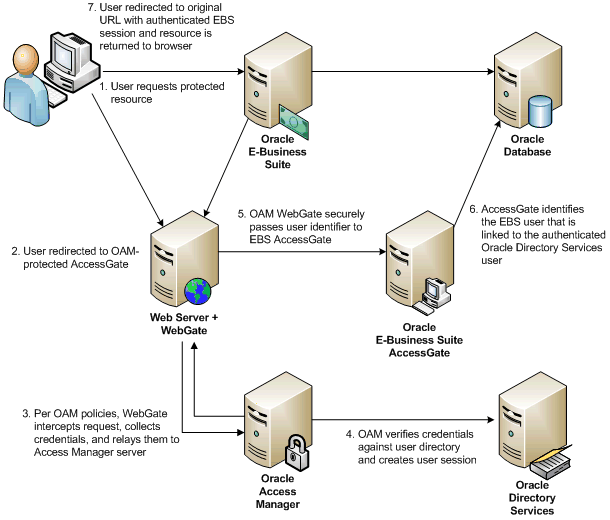


Implementing a single sign-on solution involves significant changes to the mechanism by which Oracle E-Business Suite Release 12.2 users are authenticated. Instead of authentication being performed natively, via the FND_USER table, this functionality is delegated to Oracle Single Sign-On, which can either:

- Perform user validation itself, against information stored in Oracle Directory Services.
- Delegate validation to a third-party single sign-on server.

With either of these solutions, Oracle E-Business Suite Release 12.2 accepts identities vouched for by the single sign-on mechanism. Oracle Directory Services complements this by acting as an integration point that enables Oracle E-Business Suite Release 12.2 to participate in enterprise level user management.

The sequence of actions is illustrated in the following diagram.



Additional Information: Note that where a third-party single sign-on server is in use, Oracle Access Manager and Oracle Directory Services are still required, to provide a bridge between Oracle E-Business Suite Release 12.2 and the third-party single sign-on solution.

Each Oracle E-Business Suite instance must still maintain a record of registered users, in the form of the traditional application accounts. However, the level of abstraction needed for an enterprise level user requires a mechanism that can uniquely identify a user across the enterprise. This is accomplished via a *globally unique identifier* (GUID). Oracle Directory Services and Oracle E-Business Suite store GUID information for each enterprise level user. The GUID can be considered as an identity badge that is recognized by both Oracle Directory Services and Oracle E-Business Suite.

The key role of Oracle Directory Services is to link the separate namespaces used by Oracle Access Manager and Oracle E-Business Suite. Linking the namespaces ensures that a particular user logging in via Oracle Access Manager is the same user that is represented within Oracle E-Business Suite's FND_USER repository. The linking is done by associating externally-managed Oracle Access Manager users with internally-managed Oracle E-Business Suite users via the GUIDs, which are generated by Oracle Directory Services.

In addition to this role, Oracle Directory Services has another significant part to play. While Oracle E-Business Suite is typically used mainly within an organization, certain application modules such as iRecruitment need to be available to outside users without accounts being created manually and responsibilities being assigned. This means application modules that support self-registration must create user accounts *synchronously* (in Oracle E-Business Suite and the external directory at the same time) and on demand. Oracle E-Business Suite uses specific Oracle Directory Services function calls to handle these synchronous account creation tasks.

Another requirement in such a single sign-on environment is for user enrollment to be done only once, at well defined places, with the user subsequently being known to the rest of the enterprise. Two additional features enable this:

- Support for automatic propagation of application information across an enterprise, via a *synchronization* process between Oracle Directory Services and a third-party LDAP server.
- Support for automatic propagation of user information across an enterprise, via a *provisioning* process between Oracle Directory Services and Oracle E-Business Suite Release 12.2.

User information in external, third-party user directories can be synchronized with Oracle Directory Services using the LDAP protocol. With Oracle Directory Services, customers can manage and publish user information in a central location that various application systems, including Oracle E-Business Suite, can reference.

Much of the complexity involved with integrating Oracle E-Business Suite into a single sign-on environment arises because of the need to consolidate fragmented or duplicated user data in the single sign-on environment, as a legacy of integrating previously-isolated systems.

The solution described in this chapter provides mechanisms to link the existing data together using the GUID. In addition, bulk migration tools can be used to move a large number of users between Oracle Directory Services and Oracle E-Business Suite during the transition to an integrated single sign-on environment.

Additional Information: For more information on implementing single sign-on with Oracle Single Sign-On and Oracle Directory Services, see Chapter 6 of *Oracle E-Business Suite Security Guide*, and My Oracle Support Knowledge Document 1388152.1, *Overview of Single Sign-On Integration Options for Oracle E-Business Suite.*.

Basic Single Sign-On Deployment Scenario

This section outlines a simple deployment scenario where an existing Oracle E-Business Suite instance is integrated with a new Oracle Access Manager and Oracle Directory Services infrastructure. A subsequent discussion considers additional factors, such as the existence of a third-party single sign-on solution, or the presence of multiple user repositories.

Additional Information: This section provides a high-level overview of the common tasks that will apply to all installations. The exact steps needed for the requirements of a particular site will be more detailed.

The starting point of this scenario is an existing Oracle E-Business Suite Release 12.2 installation, plus a new Oracle Access Manager and Oracle Directory Services installation on a different machine.

Oracle Directory Services has no currently existing users, apart from pre-seeded users. The requirement is to integrate Oracle E-Business Suite Release 12.2 with Oracle Access Manager and Oracle Directory Services.

Key Goals

- Oracle E-Business Suite Release 12.2 will delegate user sign-on and authentication to Oracle Access Manager
- Oracle Access Manager and Oracle E-Business Suite AccessGate will authenticate user credentials against user entries in Oracle Directory Services
- Oracle Directory Services will store every user's single sign-on account id and password

Deploying E-Business Suite with Oracle Access Manager and Oracle Directory Services

User Management Options

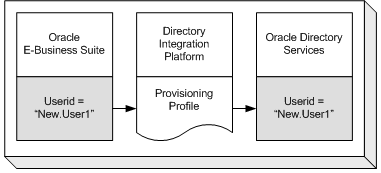
Existing Oracle E-Business Suite Release 12.2 application accounts are migrated to single sign-on accounts in Oracle Directory Services using the *Bulk Migration Tool*. After the migration, a system administrator has a number of user management options, related to the location(s) where user information is created, and where it is provisioned (sent) to.

Option 1

All user information is created in Oracle E-Business Suite Release 12.2, then provisioned into Oracle Directory Services.

- Oracle E-Business Suite Release 12.2 is configured as a *provisioning integrated application* with Oracle Directory Services
- System administrators configure the provisioning integration via *provisioning profiles*

Provisioning User Information from Oracle E-Business Suite to Oracle Directory Services



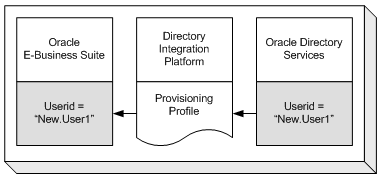
The creation of a new application account in Oracle E-Business Suite Release 12.2 will automatically trigger the creation of a new single sign-on account in Oracle Directory Services. Some of the user attributes from the application account may be provisioned in the single sign-on account in Oracle Directory Services during account creation.

Option 2

All user information is created in Oracle Directory Services, then provisioned into Oracle E-Business Suite Release 12.2:

- Oracle E-Business Suite Release 12.2 is configured as a provisioning integrated application with Oracle Directory Services
- System administrators configure the provisioning integration via *provisioning profiles*

Provisioning User Information from Oracle Directory Services to E-Business Suite



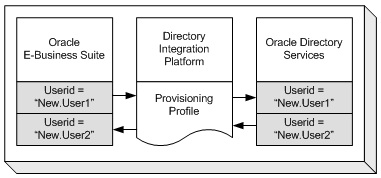
The creation of a new single sign-on account in Oracle Directory Services will automatically trigger the creation of a new application account in Oracle E-Business Suite Release 12.2. Some of the user attributes from the single sign-on account may be provisioned in the application account in Oracle Directory Services during account creation.

Option 3

All user information is created in either Oracle Directory Services or Oracle E-Business Suite Release 12.2, then provisioned into the other system:

- Oracle E-Business Suite Release 12.2 is configured as a provisioning integrated application with Oracle Directory Services
- System administrators configure the provisioning integration via provisioning profiles

Provisioning User Information Between Oracle E-Business Suite and Oracle Directory Services



The creation of a new application account in Release 12.2 will automatically trigger the creation of a new single sign-on account in Oracle Directory Services, and the creation of a new single sign-on account in Oracle Directory Services will automatically trigger the creation of a new application account in Release 12.2.

During account creation, some of the user attributes from the application account may be provisioned in the single sign-on account in Oracle Directory Services during account creation, and some of the user attributes from the single sign-on account may be provisioned in the application account in Oracle Directory Services.

Synchronizing User Attributes

For all three of the above options, a set of user attributes can, on being updated from either system, optionally be synchronized between Oracle E-Business Suite Release 12.2 and Oracle Directory Services. This is accomplished by configuring the provisioning profile.

Signing On

Attempting to gain access to an Oracle E-Business Suite Release 12.2 environment, a user who has not yet been authenticated with Oracle Single Sign-On is directed to a Single Sign-On login page, which can be customized to suit an individual site.

After authentication via Oracle Single Sign-On (or if authentication has previously been carried out) the user is redirected to the requested page or the user's home page in the Oracle E-Business Suite Release 12.2.

Signing Out

When a user logs out of an Oracle E-Business Suite instance, the user is also logged out of Oracle Access Manager and E-Business Suite AccessGate, as well as any *partner applications* that have been integrated with Oracle Access Manager. The user will see a logout page that lists all the applications he has been successfully logged out of.

Session Timeout

It is important to understand the timeout behavior of the different sessions in a single sign-on environment, to ensure the appropriate level of security is maintained.

- If a user's application session has timed out, but not his single sign-on session, he will be directed to Oracle Access Manager, and then back to Oracle E-Business Suite, without being prompted to re-authenticate.
- If a user's application session and single sign-on session have both timed out, he will be directed to the single sign-on login page to re-authenticate, and then redirected back to Oracle E-Business Suite.

Until a user's application session times out (or he explicitly logs out), he can continue to access the partner application even if his Oracle Access Manager security cookie has expired. Since the application session timeout value takes precedence over the Oracle Access Manager timeout setting, Oracle recommends setting the application session timeout value to be equal to or less than that of Oracle Access Manager.

Advanced Single Sign-On Deployment Scenarios

This section outlines four more deployment scenarios. The guidelines given should be regarded as providing a high-level strategy rather than definitive instructions, as all real world deployments will be unique, and require detailed planning. The outline solutions build upon the basic scenario discussed above.

Scenario 1

Requirement - Need to enable Oracle Access Manager with Oracle E-Business Suite Release 12.2

Starting Environment

- Multiple new Oracle E-Business Suite Release 12.2 environments have been installed
- Other than the default administrative accounts, no user accounts have been registered yet
- No single sign-on infrastructure in place

Solution

- Oracle Access Manager and Oracle Directory Services are needed for the integration required
- Oracle E-Business Suite Release 12.2 will delegate user sign-on and authentication to Oracle Access Manager
- Oracle Access Manager authenticates user credentials against user entries in Oracle Directory Services
- Oracle Directory Services contains every user's single sign-on account ID and password

Either Oracle Directory Services or one Oracle E-Business Suite Release 12.2 instance can be designated as the source of user enrollment, with the following implications:

- If Oracle Directory Services is the source, details of user accounts can be propagated to each Oracle E-Business Suite instance via the provisioning process.
- If an Oracle E-Business Suite instance is the source, the provisioning process will propagate user accounts from that instance to Oracle Directory Services, and then to the other Oracle E-Business Suite instances.

Optionally, user profile information in an Oracle E-Business Suite Release 12.2 instance can be kept synchronized with the information in Oracle Directory Services.

Scenario 2

Requirement - Need to integrate new installation of Oracle E-Business Suite Release 12.2 with existing third-party single sign-on and user directory infrastructure

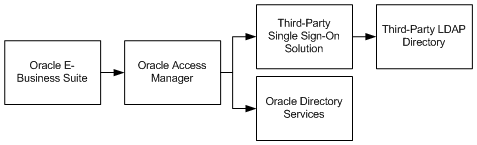
Starting Environment

- Oracle E-Business Suite Release 12.2 has been newly installed using Rapid Install.
- Other than the default administrative accounts, no user accounts have been registered yet.
- A third-party single sign-on solution is in use as a corporate single sign-on solution.
- A third-party LDAP directory is in use as a corporate user directory.

Solution

- Oracle Access Manager and Oracle Directory Services are needed for the integration.
- Oracle E-Business Suite and Oracle Access Manager must be set up so that Oracle E-Business Suite delegates authentication to Oracle Access Manager , which in turn delegates the functionality to the third-party single sign-on server in use.
- Oracle Directory Services needs to be set up to synchronize a minimal set of information from the third-party LDAP directory for all users who will access Oracle E-Business Suite via single sign-on.
- Oracle Directory Services also needs to be set up to provision users in Oracle Directory Services to Oracle E-Business Suite.

Integrating E-Business Suite with Third-Party Single Sign-On and User Directory



Existing users in the third-party LDAP directory can be bulk migrated into Oracle Directory Services, and then bulk migrated into Oracle E-Business Suite.

Optionally, user profile information in Oracle E-Business Suite can be kept synchronized with the information in the third-party LDAP directory.

Scenario 3

Requirement - Need to integrate existing Oracle E-Business Suite Release 12.2 with existing third-party single sign-on and user directory infrastructure

Starting Environment

- Oracle E-Business Suite Release 12.2 is in use, and has an up to date user repository.
- A third-party corporate single sign-on solution is in use and is to be retained.
- A third-party LDAP directory is in place as a corporate user directory and is to be retained.
- At the start of the implementation, a given user may exist in both Oracle E-Business Suite Release 12.2 and the third-party LDAP directory, with either the same user name in both or a different user name in each.

Solution

- Oracle Access Manager and Oracle Directory Services are needed for the integration.
- Oracle E-Business Suite and Oracle Access Manager need to be set up so that Oracle E-Business Suite delegates authentication to Oracle Access Manager , which in turn delegates the functionality to the third-party single sign-on server.
- Oracle Directory Services must be configured to synchronize a minimal set of information from the third-party LDAP directory for users who will access Oracle E-Business suite via single sign-on.
- Existing users in the third-party LDAP directory can be bulk migrated into Oracle Directory Services.
- Existing accounts in both Oracle E-Business Suite and the third-party LDAP directory can be linked.
- With proper planning, new users can be synchronized from the third-party LDAP directory into Oracle Directory Services, and then into Oracle E-Business Suite.
- Optionally, user profile information in Oracle E-Business Suite can be kept synchronized with the information in the third-party LDAP directory.

A simpler variant of this scenario arises when no third-party single sign-on or LDAP directory is involved. There is only an existing Oracle E-Business Suite Release 12.2 installation, plus an Oracle Access Manager and Oracle Directory Services infrastructure. In such a case, all steps relating to third-party (non-Oracle) software can be ignored.

Scenario 4

Requirement - Need to enable Oracle Single Sign-On with multiple Oracle E-Business Suite Release 12.2 installations where no Oracle Single Sign-On infrastructure is currently in place

Starting Environment

- Multiple Oracle E-Business Suite Release 12.2 instances are implemented, and each has an existing user population.
- No existing Oracle Access Manager infrastructure is in place.

Solution

- Oracle Access Manager and Oracle Directory Services are needed for the integration.

- Each Oracle E-Business Suite instance delegates user sign-on and authentication to Oracle Access Manager .
- Oracle Access Manager authenticates user credentials against user entries in Oracle Directory Services.
- Oracle Directory Services contains every user's single sign-on account id and password.
- A single sign-on account needs to be created for every user in Oracle Directory Services.
- Existing applications accounts in Oracle E-Business Suite instances need to be linked to the single sign-on account.
- Optionally, user profile information in Oracle E-Business Suite can be kept synchronized with the information in Oracle Directory Services.

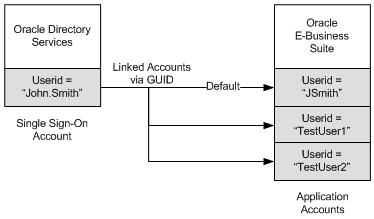
Advanced Single Sign-On Options

There are a number of advanced options that may be employed in specialized circumstances; one example is described here.

Linking Multiple Application Accounts to a Single Oracle Single Sign-On Account

Normally, a single sign-on account in Oracle Directory Services will correspond to a single application account in Oracle E-Business Suite Release 12.2. However, in special cases a user may need to have a single sign-on account in Oracle Directory Services and multiple application accounts in Oracle E-Business Suite Release 12.2.

Single Sign-On Account with Multiple Application Accounts



If required, this feature can be enabled by system administrators via the profile option 'Applications SSO Allow Multiple Accounts'.