Oracle® E-Business Suite

Security Guide

Release 12.2

Part No. E22952-39

February 2024

ORACLE

Oracle E-Business Suite Security Guide, Release 12.2

Part No. E22952-39

Copyright © 1994, 2024, Oracle and/or its affiliates.

Primary Author: Robert Farrington, Tiffany Morales Romero, Mildred Wang

Contributing Author: Erik Graversen, Elke Phelps

Contributor: Eric Bing, George Buzsaki, Anne Carlson, Steve Carter, Steven Chan, Siu Chang, Laura Chen, Kenny Tak Chi Ching, Jennifer Collins, Elanchelvan Elango, Francoise Guigues, David Kerr, Eric Locatelli, Surya Narayana Nellepalli, Emily Nordhagen, Sriram Pakanathi, Srikanth Sallaka, Renato Santis, Mike Skees, Hope Skinner-Savallisch, Jan Smith, Susan Stratton, Ashok Subramanian, Keith M. Swartz, Sukanya Tadepalli, Carol Tilley, Sanjeev Topiwala, Roger Wigenstam, Sara Woodhull

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

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.

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.

Contents

Send Us Your Comments

Preface

Part 1 Authentication and Authorization

1 Introduction to Authentication and Authorization

Access Control in Oracle E-Business Suite 1-1
Oracle User Management 1-1
Oracle Application Object Library Security 1-2

2 Access Control with Oracle User Management

Overview 2-1
Function Security 2-2
Data Security 2-3
Role Based Access Control (RBAC) 2-3
Delegated Administration 2-6
Provisioning Services 2-7
Self-Service and Approvals 2-15
Access Control With Proxy Users 2-16
The Proxy User Feature 2-16

3 Oracle User Management Setup and Administration

Setup Tasks 3-1
Defining Role Categories 3-1

Creating and Updating Roles....3-2
Security Wizard....3-3
Assigning Permissions to Roles....3-3
Searching For Assigned Roles....3-4
Diagnostics for User-Role Assignment....3-6
Creating Instance Sets and Permission Sets....3-7
Defining Delegated Administration Privileges for Roles....3-9
Defining Data Security Policies....3-14
Defining Role Inheritance Hierarchies....3-15
Creating and Updating Registration Processes....3-22
Configuring the User Name Policy....3-25
Delegated Administration Tasks....3-27
Maintaining People and Users....3-27
Creating, Inactivating, and Reactivating User Accounts....3-29
Resetting User Passwords....3-29
Unlocking Locked User Accounts....3-30
Assigning Roles to or Revoking Roles from Users....3-30
Fine Grained Access Control for Role Administration....3-31
Managing System Accounts....3-36
Registering External Organization Contacts....3-37
Registering User Accounts....3-38
Managing Proxy Users....3-41
Self Service Features....3-53
Self-Service Registration....3-54
Requesting Additional Application Access....3-54
Login Assistance....3-55
Security Reports....3-56
Home Page....3-56
Listing Functions for a User....3-57
Listing Data Security and Business Objects for a User....3-58
Listing Roles and Responsibilities for a User....3-59
Listing Users With a Given Role....3-61
Listing Functions That Can Be Accessed From a Given Role....3-62
Listing Objects for a Given Role....3-63
Listing Users for a Given Function....3-64
Listing Roles and Responsibilities for a Given Object....3-65

4 Oracle Application Object Library Security

Overview of Oracle E-Business Suite Security....4-1
HRMS Security....4-2

Enterprise Command Center Security 4-2
Oracle E-Business Suite User Passwords 4-2
Guest User Account 4-5
User Session Limits 4-5
Defining a Responsibility 4-6
Additional Notes About Responsibilities 4-6
Defining Request Security 4-7
Oracle Applications Manager Security Tests 4-10
Overview of Security Groups in Oracle HRMS 4-10
Defining Security Groups 4-10
Overview of Function Security 4-11
Terms 4-11
Executable Functions vs. Non-executable Functions 4-12
Functions, Menus, and the Navigate Window 4-13
Menu Entries with a Submenu and Functions 4-13
How Function Security Works 4-14
Implementing Function Security 4-16
Defining a New Menu Structure 4-16
Notes About Defining Menus 4-17
Menu Compilation 4-17
Preserving Custom Menus Across Upgrades 4-17
Overview of Data Security 4-18
Concepts and Definitions 4-18
Implementation of Data Security 4-21
Responsibilities Window 4-22
Security Groups Window 4-25
Users Window 4-26
Form Functions Window 4-31
Menus Window 4-36
Menu Viewer 4-39
Objects 4-40
Find Objects 4-41
Update Object 4-42
Create Object 4-42
Object Detail 4-43
Delete Object 4-44
Object Instance Sets 4-44
Manage Object Instance Set 4-44
Create Object Instance Set 4-45
Update Object Instance Set 4-46
Delete Object Instance Set 4-46

Object Instance Set Details 4-46
Grants 4-47
Search Grants 4-47
Create Grant 4-48
Define Grant 4-48
Select Object Data Context 4-48
Define Object Parameters and Select Set 4-49
Review and Finish 4-49
Update Grant 4-49
Define a Grant 4-49
View Grant 4-50
Functions 4-51
Search 4-52
Create Function 4-52
Update Function 4-53
Duplicate Function 4-53
View Function 4-54
Delete Function 4-54
Navigation Menus 4-54
Search for Menus 4-55
Create Navigation Menu 4-56
Update Menu 4-57
Duplicate Menu 4-57
View Menu 4-58
Delete Menu 4-58
Permissions 4-58
Create Permission 4-58
Update Permission 4-59
Duplicate Permission 4-59
View Permission 4-59
Delete Permission 4-60
Permission Sets 4-60
Create Permission Set 4-60
Update Permission Set 4-60
Duplicate Permission Set 4-61
View Permission Set 4-61
Delete Permission Set 4-61
Compile Security Concurrent Program 4-62
Parameter 4-62
Function Security Reports 4-62
Users of a Responsibility Report 4-63

Report Parameters 4-63
Report Heading 4-63
Column Headings 4-63
Active Responsibilities Report 4-64
Report Parameters 4-64
Report Heading 4-64
Column Headings 4-64
Active Users Report 4-65
Report Parameters 4-65
Report Heading 4-65
Column Headings 4-65
Disable and Enable Inactive FND Users Based on Security User Type 4-66
Reports and Sets by Responsibility Report 4-66
Report Parameters 4-67
Report Headings 4-67
Oracle Application Object Library REST Security Services 4-67
Cookie Domain Scoping 4-79
Allowed Resources 4-82
Allowed Redirects 4-101

5 Single Sign-On Integration

Overview of Single Sign-On Integration 5-1
Introduction to Enterprise User Management 5-3
Integration Actions and Options 5-4
Enterprise User Management 5-11
Deployment Scenario 0: E-Business Suite + SSO and Oracle Directory Services 5-15
User Management Options 5-16
End-User Experience 5-18
Session Timeout Behavior 5-20
User Management Options 5-21
Critical Implementation Decisions 5-27
Implementation Instructions 5-28
Deployment Scenario 1: Multiple Oracle E-Business Suite Instances + Central SSO and Oracle Directory Services Instance 5-30
Deployment Scenario 2: New Oracle E-Business Suite Installation + Existing Third-Party Identity Management Solution 5-32
End-User Experience 5-33
User Management 5-34
Critical Implementation Decisions 5-36
Implementation Instructions 5-37
Deployment Scenario 3: Existing Oracle E-Business Suite Instance + Existing Third-Party

Identity Management Solutions 5-38
Critical Implementation Decisions 5-43
Implementation Instructions 5-44
Deployment Scenario 4: Multiple Oracle E-Business Suite Instances with Unique User Populations 5-45
Advanced Features 5-46
Single Sign-On Profile Options 5-52
Configuring Directory Integration Platform Provisioning Templates 5-66
Administering the Provisioning Process 5-70
Changing E-Business Suite Database Account Password 5-74
Manual Subscription Management With Provsubtool 5-76
Migrating Data Between Oracle E-Business Suite and Oracle Directory Services 5-78
Enabling and Disabling Users 5-91
Synchronizing Oracle HRMS with Oracle Directory Services 5-92
Supported Attributes 5-93
FND_SSO_UTIL Procedures 5-96
References and Resources for Single Sign-On 5-97
Glossary of Terms 5-97

Part 2 Secure Configuration

6 Overview of Secure Configuration

About Oracle E-Business Suite Secure Configuration 6-1
System-Wide Advice 6-3
Differences Between Oracle E-Business Suite Releases 6-4

7 Oracle TNS Listener Security

About Oracle TNS Listener Security 7-1
Hardening 7-1
Network 7-5
Authorization 7-9
Audit 7-9

8 Oracle Database Security

About Oracle Database Security 8-1
Hardening 8-1
Authentication 8-2
Authorization 8-4

9 Oracle Application Tier Security

About Oracle Application Tier Security 9-1
Hardening 9-1
Authorization 9-2
Network 9-3

10 Oracle E-Business Suite Security

About Oracle E-Business Suite Security 10-1
Hardening 10-1
Network 10-9
Authentication 10-19
Authorization 10-29

11 Desktop Security

About Desktop Security 11-1
Hardening 11-1

12 Operating Environment Security

Overview of Operating Environment Security 12-1
Hardening 12-1
Network 12-3
Authentication 12-7
Authorization 12-8
Maintenance 12-9

13 Secure Configuration Console

Overview 13-1
Using the Secure Configuration Console 13-2

Part 3 Guidelines for Auditing and Logging

14 Introduction to Guidelines for Auditing and Logging

About Auditing and Logging 14-1
Why Audit? 14-1

15 Auditing and Logging Features in Oracle E-Business Suite

Overview of Features 15-1

Recent and Current Activity....15-1
Historical Activity....15-2
Unexpected Events....15-3
Oracle E-Business Suite Auditing Scripts....15-3

16 Using Oracle E-Business Suite Application Auditing and Logging Features

Introduction....16-1
Unsuccessful Login Attempts....16-1
Data Changes Tracked with Who Columns....16-1
Sign-On Audit....16-3
Enabling Sign-On Audit....16-4
Disabling Inactive Sessions....16-7
Purging Session Information....16-8
Purging Sign-On Audit Data....16-8
Sign-On Audit Reports....16-9
Session Audit Information....16-9
Page Access Tracking....16-10
Database Connection Tagging....16-14
Debug Logging (Unexpected Logging)....16-15
Oracle E-Business Suite Audit Trail....16-16

17 Oracle E-Business Suite Technology Stack Auditing and Logging Features

Introduction....17-1
Application Tier Technology Stack....17-1
Format of the Listener Log Audit Trail....17-5
Database Alert Log....17-6
Database Auditing....17-6
Optional Oracle Technology Integrations....17-7

18 Enabling Oracle E-Business Suite Audit Trail

Overview....18-1
Steps to Enable Audit Trail....18-2
Audit Trail Shadow Tables, Triggers, and View....18-5
Purging Audit Trail Records....18-7
Disabling an Enabled Audit Trail....18-8
Restarting an Audit....18-9
Tables....18-10
Reporting on Audit Data....18-14
Implications of Upgrading an Audit Trail....18-14
Disabling Audit Trail....18-14

Additional Audit Trail Reporting 18-16
Audit Industry Template 18-16
Audit Hierarchy Navigator 18-17
Audit Query Navigator 18-19
Audit Report 18-20
Monitor Users Window 18-21
Audit Installations Window 18-23
Audit Groups Window 18-25
Audit Tables Window 18-27
Audit Trail Search Pages 18-30

A Running Web Scanning Tools

Overview A-1
Preparing Your Oracle E-Business Suite System for the Web Scan A-1
Reviewing the Results A-2

B Database Schemas Found in Oracle E-Business Suite

Table of Database Schemas in Oracle E-Business Suite B-1

C Processes Used by Oracle E-Business Suite

Table of Processes Used by Oracle E-Business Suite C-1

D Ports Used by Oracle E-Business Suite

Table of Ports Used by Oracle E-Business Suite D-1
Table of Ports Used by WebLogic Server D-3

E Security Checklist

About the Security Checklist E-1
Overview E-1
Oracle TNS Listener Security E-2
Oracle Database Security E-2
Oracle Application Tier Security E-3
Oracle E-Business Suite Security E-3
Desktop Security E-5
Operating Environment Security E-5

F Sign-On Audit Concurrent Manager Reports

About Sign-On Audit Concurrent Manager Reports F-1
Sign-On Audit Concurrent Requests Report F-1

Sign-On Audit Forms Report F-3
Sign-On Audit Responsibilities Report F-6
Sign-On Audit Unsuccessful Logins Report F-8
Sign-On Audit Users Report F-10

G Additional References

References G-1

H Security Features for Earlier Oracle E-Business Suite Releases

Overview H-1
FND: Security Resource Logging Profile Option Values for Earlier Releases H-1
Obsolete Secure Configuration Console Checks H-2

Index

Send Us Your Comments

Oracle E-Business Suite Security Guide, Release 12.2

Part No. E22952-39

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document. Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

Note: Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the new Oracle E-Business Suite Release Online Documentation CD available on My Oracle Support and www.oracle.com. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: appsdoc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at www.oracle.com.

Preface

Intended Audience

Welcome to Release 12.2 of the *Oracle E-Business Suite Security Guide.*

This guide assumes you have a working knowledge of the following:

- The principles and customary practices of your business area.
- Computer desktop application usage and terminology.

If you have never used Oracle E-Business Suite, we suggest you attend one or more of the Oracle E-Business Suite training classes available through Oracle University.

> **Note:** This book typically uses UNIX nomenclature in specifying files and directories. Windows users should substitute the appropriate Windows terms where applicable. For example, a UNIX .env (environment) file will be a .cmd (command) file on Windows.

See Related Information Sources on page xviii for more Oracle E-Business Suite product information.

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.

Structure

1 Introduction to Authentication and Authorization
2 Access Control with Oracle User Management
3 Oracle User Management Setup and Administration
4 Oracle Application Object Library Security
5 Single Sign-On Integration
6 Overview of Secure Configuration
7 Oracle TNS Listener Security
8 Oracle Database Security
9 Oracle Application Tier Security
10 Oracle E-Business Suite Security
11 Desktop Security
12 Operating Environment Security
13 Secure Configuration Console
14 Introduction to Guidelines for Auditing and Logging
15 Auditing and Logging Features in Oracle E-Business Suite
16 Using Oracle E-Business Suite Application Auditing and Logging Features
17 Oracle E-Business Suite Technology Stack Auditing and Logging Features
18 Enabling Oracle E-Business Suite Audit Trail
A Running Web Scanning Tools
B Database Schemas Found in Oracle E-Business Suite
C Processes Used by Oracle E-Business Suite
D Ports Used by Oracle E-Business Suite
E Security Checklist
F Sign-On Audit Concurrent Manager Reports
G Additional References
H Security Features for Earlier Oracle E-Business Suite Releases

Related Information Sources

This book is included in the Oracle E-Business Suite Documentation Library. If this guide refers you to other Oracle E-Business Suite documentation, use only the latest Release 12.2 versions of those guides.

Online Documentation

All Oracle E-Business Suite documentation is available online (HTML or PDF).

- **Online Help** - Online help patches (HTML) are available on My Oracle Support.
- **Oracle E-Business Suite Documentation Library** - This library, which is included in the Oracle E-Business Suite software distribution, provides PDF documentation as of the time of each release.
- **Oracle E-Business Suite Documentation Web Library** - This library, available on the Oracle Help Center (https://docs.oracle.com/cd/E26401_01/index.htm), provides

the latest updates to Oracle E-Business Suite Release 12.2 documentation. Most documents are available in PDF and HTML formats.

- **Release Notes** - For information about changes in this release, including new features, known issues, and other details, see the release notes for the relevant product, available on My Oracle Support.

- **Oracle Electronic Technical Reference Manual -** The Oracle Electronic Technical Reference Manual (eTRM) contains database diagrams and a detailed description of database tables, forms, reports, and programs for each Oracle E-Business Suite product. This information helps you convert data from your existing applications and integrate Oracle E-Business Suite data with non-Oracle applications, and write custom reports for Oracle E-Business Suite products. The Oracle eTRM is available as an application in Oracle E-Business Suite.

Related Guides

You should have the following related books on hand. Depending on the requirements of your particular installation, you may also need additional manuals or guides.

Oracle Application Framework Developer's Guide

This guide contains the coding standards followed by Oracle E-Business Suite Development to create applications with Oracle Application Framework. This guide is available in PDF format on My Oracle Support, and as online documentation in JDeveloper 10g with Oracle Application Extension.

Oracle E-Business Suite Cloud Manager Guide

This guide describes how to manage Oracle E-Business Suite environments on Oracle Cloud Infrastructure (OCI) using the automated tooling in Oracle E-Business Suite Cloud Manager.

Oracle E-Business Suite Concepts

This book is intended for all those planning to deploy Oracle E-Business Suite Release 12.2, or contemplating significant changes to a configuration. After describing the Oracle E-Business Suite architecture and technology stack, it focuses on strategic topics, giving a broad outline of the actions needed to achieve a particular goal, plus any installation and configuration choices that are available.

Oracle E-Business Suite Developer's Guide

This guide contains the coding standards followed by Oracle E-Business Suite Development. It describes the Oracle Application Object Library components needed to implement the Oracle E-Business Suite user interface described in the *Oracle E-Business Suite User Interface Standards for Forms-Based Products*. It provides information to help you build your custom Oracle Forms Developer forms so that they integrate with Oracle E-Business Suite. In addition, this guide has information for customizations in features such as concurrent programs, flexfields, messages, and logging.

Oracle E-Business Suite Electronic Technical Reference Manual User's Guide

This guide describes how to set up and navigate Oracle E-Business Suite Electronic Technical Reference Manual (eTRM) user interface in Oracle E-Business Suite. It also explains how to browse and search the Oracle eTRM repository to locate desired FND and database metadata and objects, and how to view object details, reports, and diagrams.

Oracle E-Business Suite Installation Guide: Using Rapid Install

This book describes how to run Rapid Install to perform a fresh installation of Oracle E-Business Suite Release 12.2 or to replace selected technology stack executables in an existing instance.

Oracle E-Business Suite Maintenance Guide

This guide explains how to patch an Oracle E-Business Suite system, describing the adop patching utility and providing guidelines and tips for performing typical patching operations. It also describes maintenance strategies and tools designed to help keep a system running smoothly.

Oracle E-Business Suite Mobile Apps Administrator's Guide, Release 12.1 and 12.2

This guide includes the latest mobile release with new underlying technologies, as well as the earlier mobile releases built with Oracle Mobile Application Framework (MAF). It explains how to set up an Oracle E-Business Suite instance to support connections from Oracle E-Business Suite mobile apps. It also describes common administrative tasks for configuring Oracle E-Business Suite mobile apps. Logging and troubleshooting information is also included in this book.

Oracle E-Business Suite Mobile Apps Developer's Guide, Release 12.1 and 12.2

This guide includes information for the latest mobile release with new underlying technologies, as well as the earlier mobile releases built with Oracle Mobile Application Framework (MAF). For mobile releases built with MAF, this guide describes how to develop enterprise-distributed mobile apps by using mobile application archive (MAA) files and how to implement corporate branding. It also explains required tasks on implementing push notifications for supported mobile apps. In addition, it includes how to implement Oracle E-Business Suite REST services to develop custom mobile apps by using the Login component from Oracle E-Business Suite Mobile Foundation or using any mobile app development framework if desired.

Oracle E-Business Suite Setup Guide

This guide contains information on system configuration tasks that are carried out either after installation or whenever there is a significant change to the system. The activities described include defining concurrent programs and managers, enabling Oracle Applications Manager features, and setting up printers and online help.

Oracle E-Business Suite User's Guide

This guide explains how to navigate products, enter and query data, and run concurrent requests by means of the user interfaces (UI) of Oracle E-Business Suite. It includes basic information on setting preferences and customizing the UI. An introduction to Oracle Enterprise Command Centers is also included. Lastly, this guide

describes accessibility features and keyboard shortcuts for Oracle E-Business Suite.

Integration Repository

The Oracle Integration Repository is a compilation of information about the service endpoints exposed by the Oracle E-Business Suite of applications. It provides a complete catalog of Oracle E-Business Suite's business service interfaces. The tool lets users easily discover and deploy the appropriate business service interface for integration with any system, application, or business partner.

The Oracle Integration Repository is shipped as part of the Oracle E-Business Suite. As your instance is patched, the repository is automatically updated with content appropriate for the precise revisions of interfaces in your environment.

Do Not Use Database Tools to Modify Oracle E-Business Suite Data

Oracle STRONGLY RECOMMENDS that you never use SQL*Plus, Oracle Data Browser, database triggers, or any other tool to modify Oracle E-Business Suite data unless otherwise instructed.

Oracle provides powerful tools you can use to create, store, change, retrieve, and maintain information in an Oracle database. But if you use Oracle tools such as SQL*Plus to modify Oracle E-Business Suite data, you risk destroying the integrity of your data and you lose the ability to audit changes to your data.

Because Oracle E-Business Suite tables are interrelated, any change you make using an Oracle E-Business Suite form can update many tables at once. But when you modify Oracle E-Business Suite data using anything other than Oracle E-Business Suite, you may change a row in one table without making corresponding changes in related tables. If your tables get out of synchronization with each other, you risk retrieving erroneous information and you risk unpredictable results throughout Oracle E-Business Suite.

When you use Oracle E-Business Suite to modify your data, Oracle E-Business Suite automatically checks that your changes are valid. Oracle E-Business Suite also keeps track of who changes information. If you enter information into database tables using database tools, you may store invalid information. You also lose the ability to track who has changed your information because SQL*Plus and other database tools do not keep a record of changes.

Part 1

Authentication and Authorization

1

Introduction to Authentication and Authorization

Access Control in Oracle E-Business Suite

This release of Oracle E-Business Suite includes a sophisticated security system. Core Security includes a Role Based Access Control model that builds on the Function Security and Data Security models. A set of administrative features that build on Core Security are also provided.

Oracle User Management

Oracle User Management is a secure and scalable system that enables organizations to define administrative functions and manage users based on specific requirements such as job role or geographic location. With Oracle User Management, instead of exclusively relying on a centralized administrator to manage all its users, an organization can create local administrators and grant them sufficient privileges to manage a specific subset of the organization's users. This provides the organization with a more granular level of security, and the ability to make the most effective use of its administrative capabilities.

Oracle's function and data security models constitute the base layers of this system, and contain the traditional system administrative capabilities. Organizations can optionally add more layers to the system, depending on the degree of flexibility they require.

Key features of Oracle User Management include:

- **Role Based Access Control (RBAC)** - Enables organizations to create roles based on specific job functions, and to assign these roles the appropriate permissions. With RBAC, administrative privileges and user access are determined by assigning individuals the appropriate roles.

- **Delegated Administration** - Enables system administrators to delegate some of their administrative privileges to individuals that manage a subset of the

organization's users. These individuals are assigned administrative privileges for a limited set of roles that they can assign to the users they manage.

- **Registration Processes** - Enable organizations to provide end-users with a method for requesting various levels of access to the system, based on their eligibility. Registration processes also simplify an administrator's job by providing streamlined flows for account maintenance and role assignment.

- **Self Service Requests and Approvals** - Enable end users to request initial access or additional access to the system.

Oracle User Management is used in both an administrative and a functional capacity. System administrators use Oracle User Management to define the available levels of access control as required, including RBAC, Delegated Administration, Registration Processes, and Self Service & Approvals. Part of this setup includes defining local administrators primarily by creating administrative roles and assigning them to individuals who serve as an organization's local administrators. Once this is accomplished, local administrators use Oracle User Management to manage a subset of an organization's users.

Oracle Application Object Library Security

Oracle Application Object Library security comprises two main components, Function Security and Data Security.

Function Security restricts user access to individual menus of functions, such as forms, HTML pages, or widgets within an application. Function Security by itself restricts access to various functions, but it does not restrict access to the data a user can see or what actions a user can perform on that data.

Data Security restricts the access to the individual data that is shown once a user has selected a menu or menu option. For example, with Data Security you can control the set of users that a particular local security administrator can access within Oracle User Management. In conjunction with Function Security, Data Security provides additional access control on data that a user can see or actions a user can perform on that data.

2

Access Control with Oracle User Management

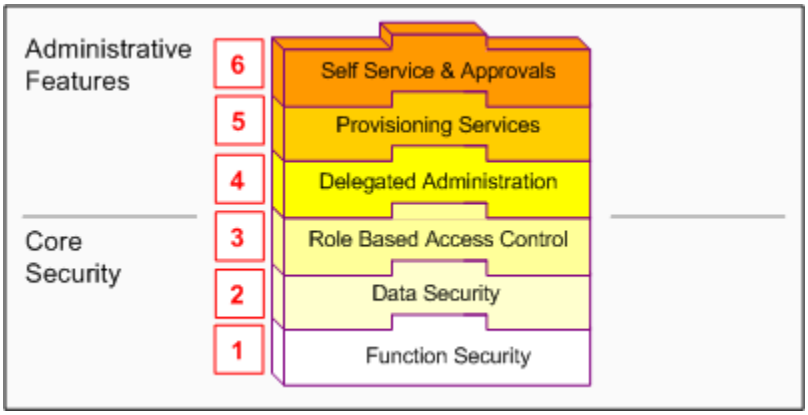
Overview

This chapter introduces the Core Security and Administrative Features of Oracle User Management. Core Security includes Oracle's Function and Data Security models, as well as Role Based Access Control. Administrative Features build upon Core Security and include Delegated Administration, Registration Processes, and Self Service and Approvals.

Core Security and Administrative Features are implemented in successive layers and each builds upon the one that precedes it. Organizations can optionally uptake the various layers, depending on the degree of automation and scalability that they wish to build upon the existing Function and Data Security models.

In general, Access Control with Oracle User Management begins with basic system administration tasks, progresses to more distributed, local modes of administration, and ultimately enables users to perform some basic, predefined registration tasks on their own. The following diagram illustrates how the layers build upon each other.

Oracle User Management Layers



Oracle User Management provides support for legacy and application-specific security mechanisms through workflow business events. Oracle User Management raises these events once a user's request is approved. Organizations can then intercept these events, determine the appropriate action, and assign any additional privileges that may be required.

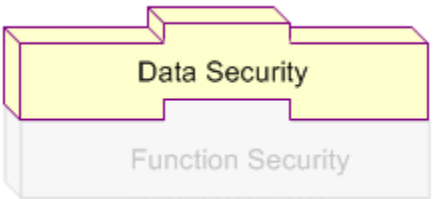
Function Security

Function Security Layer

Function Security is the base layer of access control in Oracle E-Business Suite. It restricts user access to individual menus and menu options within the system, but does not restrict access to the data contained within those menus. For example, an organization could use Function Security to provide its sales representatives with the required menus and menu options for querying customers. It could also control access to specific components of those pages such as a button on a sales forecasting page. For a more comprehensive explanation of function security, see: Oracle Application Object Library Security, page 4-1.

Data Security

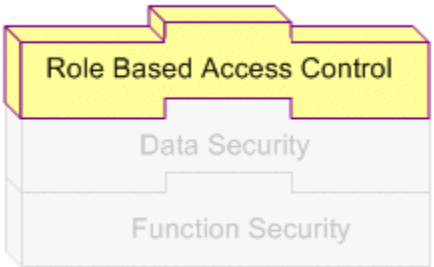
Data Security Layer



Data Security is the next layer of access control. Building on Function Security, Data Security provides access control within Oracle E-Business Suite on the data a user can access, and the actions a user can perform on that data. Oracle E-Business Suite restricts access to individual data that is displayed on the screen once the user has selected a menu or menu option. For example, Data Security restricts the set of users that a local administrator can access within Oracle User Management. Data Security policies can only be defined for applications that have been written to utilize the Data Security Framework. For a more comprehensive explanation of data security, see Oracle Application Object Library Security, page 4-1.

Role Based Access Control (RBAC)

Role Based Access Control Layer



RBAC is the next layer and builds upon Data Security and Function Security. With RBAC, access control is defined through roles, and user access to Oracle E-Business Suite is determined by the roles granted to the user. Access control in Oracle E-Business Suite closely follows the RBAC ANSI standard (ANSI INCITS 359-2004) originally proposed by the US National Institute of Standards & Technology (NIST), which

defines a role as "a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role."

A role can be configured to consolidate the responsibilities, permissions, function security and data security polices that users require to perform a specific function. This is accomplished with a one-time setup, in which permissions, responsibilities, and other roles are assigned to the role. Users are not required to be assigned the lower-level permissions directly, since permissions are implicitly inherited on the basis of the roles assigned to the user. This simplifies mass updates of user permissions, since an organization need only change the permissions or role inheritance hierarchy defined for a given role, and the users assigned that role will inherit the new set of permissions automatically.

Organizations can define roles that closely mirror their business situation. For example, an organization can create an "Employee" role and then assign that role to all of its employees. It can also create an "External" role and assign that role to customers and suppliers. Further examples may include specific roles such as "Support Agent," "Sales Rep," "Sales Managers." In these examples, each role contains a specific level of access privileges that restricts its assignees to the scope of their job functions. Some members of the organization will probably be assigned more than one role. A sales representative would be assigned the Employee and Sales Representative roles, and a Sales Manager would be assigned the Employee, Sales Representative, and Sales Manager roles. Roles and role assignments are stored in the workflow directory, which is interpreted by the security system at runtime.

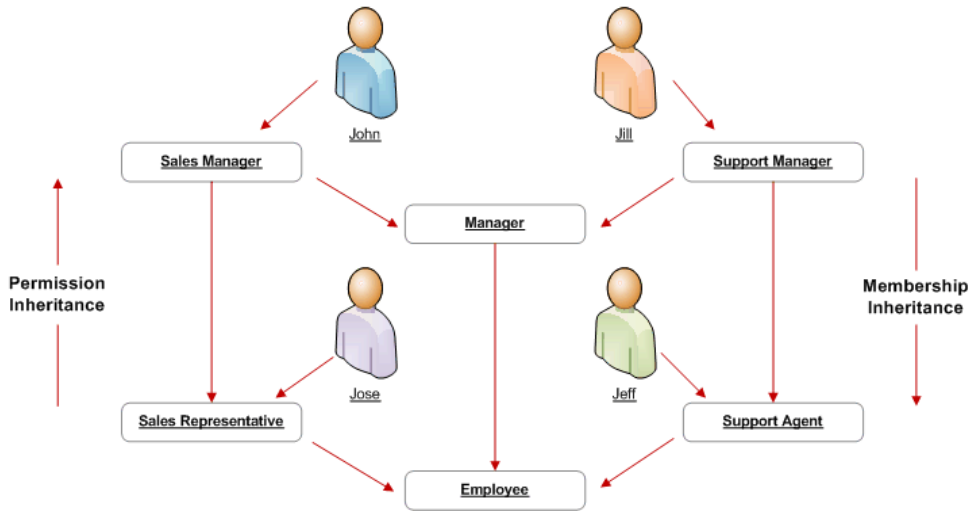
Role Categories

As part of the Oracle E-Business Suite RBAC model, Oracle User Management introduces Role Categories. Administrators can create role categories to bundle roles and responsibilities to make the process of searching for roles and responsibilities easier. For example, all sales and marketing related roles could be included in the Sales & Marketing category.

Role Inheritance Hierarchies

Roles can be included in role inheritance hierarchies that can contain multiple subordinate roles and superior roles. With role inheritance hierarchies, a superior role inherits all of the properties of its subordinate role, as well as any of that role's own subordinate roles. The following example demonstrates how role inheritance hierarchies can greatly simplify user access control and administration.

Role Inheritance Hierarchy



In the above figure, the arrows on each side of the diagram indicate membership inheritance and permission inheritance. Text in the rounded boxes indicates roles. An arrow pointing from an individual to a role indicates that this individual is assigned the role. An arrow pointing from one role to another indicates that the role from which the arrow points is the superior role, and the role to which it points is the subordinate role. Permissions associated with a role are inherited by all of its superior roles and the individuals to which any of these roles are assigned.

In this example, some roles such as "Employee" or "Manager" are assigned general permissions for a given function. For example, the Employee role may provide access to menus generally available to all employees, while the Manager role provides access to menus that should only be viewed by managers. Because the Employee role is a subordinate role of the Manager role, anyone assigned the Manager role automatically obtains the permissions associated with the Employee role. Other roles in this example pertain to more specific job functions, such as Sales Manager and Sales Representative, or Support Manager and Support Agent. These roles may provide access to job-specific menus and data such as the Sales Forecasting menu, or the Support application.

Delegated Administration

Delegated Administration Layer

Delegated Administration is a privilege model that builds on the RBAC system to provide organizations with the ability to assign the required access rights for managing roles and user accounts. With delegated administration, instead of relying on a central administrator to manage all its users, an organization can create local administrators and grant them sufficient privileges to manage a specific subset of the organization's users and roles. This provides organizations with a tighter, more granular level of security, and the ability to easily scale their administrative capabilities. For example, organizations could internally designate administrators at division or even department levels, and then delegate administration of external users to people within those (external) organizations. Delegation policies are defined as data security policies. The set of data policies that are defined as part of delegated administration are known as Administration Privileges.

A delegated administrator can be given the capability to perform one or more of the following role management actions: Create Role, Manage Role, Manage Role Hierarchy, Run Security Wizard, Assign Role, and Revoke Role. Older releases required delegated administrators to be given either all role management privileges, or none. Now the administration operations have been separated, so the super administrator can specify which operations can be performed by which delegated administrator on which set of roles.

Administration Privileges

Administration Privileges determine the users, roles and organization information that delegated administrators (local administrators) can manage. Each privilege is granted separately, yet the three work in conjunction to provide the complete set of abilities for the delegated administrator.

- **User Administration Privileges** A local administrator must be granted User Administration Privileges to determine the users and people the local administrator can manage. Local administrators can be granted different privileges for different subsets of users. For example, a local administrator can be granted privileges only to query one set of users, and granted full privileges (including update and reset password) for another set. Local administrators cannot query users for which they do not have administration privileges.

- **Role Administration Privileges** Role Administration Privileges define the roles that local administrators can directly assign to and revoke from the set of users they manage.

- **Organization Administration Privileges** Organization Administration Privileges define the external organizations a local administrator can view in Oracle User Management. This privilege enables an administrator to search for people based on their organization, if the local administrator has additionally been granted access to view the people in that organization (User Administration Privileges). Depending on the user administration privileges, an administrator may have the ability to register new people for that organization.

Oracle E-Business Suite continues to support the traditional "System Administrator" level of administration privileges, where a designated group of people manages all users and access privileges. Oracle User Management ships a predefined Security Administrator role, which gives the administrator the privileges to manage all users including system accounts and all roles in the system.

Delegated administration setup for User Administration requires the creation of instance sets and permission sets. Instance sets can be created from the main UMX screen. All possible combinations of seeded UMX permissions are seeded as permission sets and made available from this screen. A data security object, UMX_SYS_ACCT, represents system accounts. Administrators can create instance sets against this object to specify system accounts that can be managed.

Provisioning Services

Provisioning Services Layer

Provisioning services are modeled as *registration processes* that enable end users to perform some of their own registration tasks, such as requesting new accounts or additional access to the system. They also provide administrators with a faster and more efficient method of creating new user accounts, as well as assigning roles. Registration processes accomplish this by encapsulating core components of registration, including:

- The role(s) assigned after the user successfully completes the process.
- An optional registration user interface for collecting account or additional information.
- A workflow for approval, confirmation, rejection, and identity verification notifications.
- The Approval Management Transaction Type. A transaction type represents a set of approval routing rules that are interpreted at runtime.
- The set of users that are eligible to sign up for additional access (only applicable for Request for Additional Access registration processes).
- Whether identity verification is required. Identity verification confirms the identity of a requester before the registration request is processed, by sending an email notification to the requester's email address. If the recipient does not reply within a specified time, the request will be automatically rejected.
- The set of local administrators that should be able to register people and/or create users through the Account Creation by Administrators registration process.

When a user completes registration using a registration process, the system captures the required information from the user, and subsequently assigns that person a new user account, role, or both. Oracle User Management supports three types of registration processes: Self-service Account Requests, Requests for Additional Access, and Account Creation by Administrators.

Self-Service Account Requests

Commonly referred to as Self-Service Registration, self-service account requests provide a method for individuals to request a new user account. Consider a case where customers may need to register before they can purchase an item from an online store. Once the registration process has been completed, the customer obtains both a user account and the necessary role(s) for accessing some portion of the web site in which they registered.

Oracle User Management provides sample self-service registration UIs for internal employees, and for new, external individuals. Organizations can copy these sample self-service registration UIs and extend them based on their own requirements. In addition, organizations that wish to support other types of users, or capture additional

information specific to their applications, are able to extend or create their own registration UIs and business logic.

Oracle User Management provides support for displaying different registration links on the login page based on the application tier login page that provides access. The registration link can contain additional parameters that are not known at design time, such as the country code. These additional parameters can be used later during the registration process. Using country code as an example, a registration process could route the approval requests to the most appropriate approver. Therefore, all those who request an account from Norway could be routed to a Norwegian account approver.

> **Additional Information:** "Accounts" and "User Accounts" refer to login accounts, stored in the FND_USER table.

Requests for Additional Access

Users can request additional access through the Oracle User Management Access Request Tool (ART), available in the Global Preferences menu. Requests for Additional Access uses the same Oracle User Management infrastructure and processing logic as Self Service Account Requests.

Additional Access and Self Service Eligibility

Eligibility defines the Roles for which a user can sign up using the Access Request Tool. It determines the groups of users defined in the workflow directory that are entitled to register for a given role. A registration process of type "Additional Access" can be made available to predefined sets of users across all roles or groups. Eligibility is defined as a data security policy, and interrogated at runtime by the Access Request Tool.

Because roles are stored in the workflow directory, they can be used both to grant access to applications and to define eligibility. This enables organizations to define an incremental registration process in which new users can sign up for roles if they are first approved for the ones that precede them. For example, once a new user is approved for the A Role, the user can then sign up for the B Role. If, however, the user is not first approved for the A Role, then the user cannot sign up for the B Role.

Oracle User Management can define eligibility policies for any groups and roles stored in the workflow directory.

Delegated Administration and Registration Processes

When an administrator assigns a role to a user, the administrator essentially fulfills a registration request on behalf of the user. When the administrator assigns a role to the user, Oracle User Management invokes the corresponding "Additional Access (Administrator)" registration process (if defined) and interprets the registration processes metadata. If a registration UI is defined, Oracle User Management launches it and the administrator completes the registration process. Notification workflows are only invoked when a registration process is defined for the role that is being assigned to the user.

Directly assigning a role to a user bypasses any pre-defined approval routing rules, as defined in Oracle Approval Management. Administrators can view all roles that are assigned to a user, but cannot assign or revoke roles for which they do not have administrative privileges. An administrator assigning a role to a user is essentially fulfilling a registration request on behalf of the user.

Account Creation By Administrators

Administrators benefit from registration processes having been designed to streamline the process of creating and maintaining user access. Registration processes of this type are geared toward administrators, especially delegated administrators, to ensure consistent application of the organization's user security policies. Each account creation registration process can be made available to selected administrators.

Registration Process Infrastructure

This section describes components of the common infrastructure that handles all registration requests submitted through Oracle User Management.

User Name Policies

Oracle User Management enables organizations to define their own user name policies for new users. These can include such formats as email address, "firstname.lastname" (or an abbreviated version), employee number, social security number, or some other meaningful information. When the account request is submitted, Oracle User Management reserves the specified user name for the duration of the approval process.

Oracle User Management ships with a default user name policy that identifies users by their *email address*. This is implemented as a configurable infrastructure that organizations can easily customize to suit their specific needs.

Email Verification

Oracle User Management provides a mechanism for verifying the identity of the requester before the registration request is processed. Identity verification is based on the email address provided by the requester. Oracle User Management sends the requester an email notification when the requester has completes the registration flow. If the user does not reply to the email notification within a specified time, the request is automatically rejected. Email verification is only applicable to Self-Service account requests, and is enabled or disabled for each registration process.

> **Note:** Oracle recommends that when building self-service registration UIs with identity verification enabled, an organization should indicate in the UIs and confirmation messages that a response is required to process the user's request.

Temporary Storage of Registration Data

Oracle User Management provides a mechanism to store registration data in a pending state until a request is approved. This data is available to the workflow notifications used for sending approvals, to Approval Management routing rules, and to the business logic that writes the information in the final destination tables. Oracle User Management accomplishes this by using event objects that are part of the Workflow Business Events infrastructure.

Registration Engine

The Oracle User Management registration engine uses a workflow to define the business logic that drives the registration process once a request has been submitted. The name of the workflow is UMX Registration Workflow (UMXREGWF).

This process:

- Raises business events
- Provides temporary storage of registration data
- Provides identity verification
- Includes the integration point with Oracle Approval Management
- Activates user accounts
- Reserves and releases user names
- Assigns roles
- Maintains registration status in the Oracle User Management schema
- Launches notification workflows

Organizations can customize the components of the registration process (such as notifications, approval routing rules, and user name policies) without having to review and understand all Oracle User Management code.

Routing Approval Requests

Approvers can be configured based on rules that are specific to each type of request. Organizations can define these rules according to their requirements, and can specify types of requests that do not require approval. Oracle User Management is integrated with Oracle Approval Management, an application that provides a flexible and powerful rules engine that can be configured through declarative means to route approval requests. Oracle User Management also provides APIs that enable approval rules to be based on any information captured during the registration process, including any parameters passed from the "Register Here" link on the Login page, which may not have been known at design time.

Workflow Business Events

Oracle User Management raises the following Workflow business events:

Oracle User Management Workflow Business Events

Event	Description
oracle.apps.fnd.umx.rolerequested	An event that is raised when a role is requested.
oracle.apps.fnd.umx.accountrequested	An event that is raised when an account is requested.
oracle.apps.fnd.umx.requestapproved	An event that is raised when an account or role is approved.
oracle.apps.fnd.umx.requestrejected	An event that is raised when an account or role is rejected.
<custom event>	A custom business event is raised for the owner of the registration process to write the registration. The custom event is raised multiple times. For more information, see My Oracle Support Knowledge Document 399400.1, *Oracle Applications User Management (UMX) Developer's Guide*.

> **Note:** Oracle recommends using the UMX events mentioned above only for centralized requirements such as auditing. For any registration-specific processing, use the custom event defined for the registration process.

Depending on the context, the event parameters listed in the following table are set automatically by the Oracle User Management registration engine when business events are raised. Any additional information captured in the registration UI, approval notifications, or programmatically through business logic is also available as event parameters.

Oracle User Management Workflow Business Event Parameters

Name	Description
REG_SERVICE_CODE	Represents the primary key of the registration process
REG_SERVICE_TYPE	The type of registration process
REQUESTED_BY_USER_ID	Identifies the user submitting the request
REQUESTED_FOR_USER_ID	Identifies the user for whom the request is submitted
REQUESTED_USERNAME	The requested user name
WF_ROLE_NAME*	Represents the primary key value of the requested role or the default role for any account requests
AME_TRANSACTION_TYPE_ID	Represents part of the primary key for the transaction type in Oracle Approval Management
AME_APPLICATION_ID	Represents part of the primary key for the transaction type in Oracle Approval Management

* WF_ROLE_NAME is not required for Self Service Account Creation or Account Creation for Administrators registration processes. In such cases, a null value is passed. Any additional information captured in the registration UI, from approvers, in approval notifications, or set by business logic is also available as parameters when an Oracle User Management business event is raised.

Sample Program

```
/*************************************************************
This is a sample subscription to any of the above events.

Function custom_logic (p_subscription_guid in raw,
 p_event in out NOCOPY WF_EVENT_T)
Return varchar2 is
 l_first_name varchar2(30);
Begin
 l_first_name :=  p_event.getvalueforparameter ('FIRST_NAME');
// Manipulate the data
End custom_logic;
*************************************************************/
```

Registration Status

Users can check registration status of requests through the Access Request Tool (ART) and administrators can do so using the Administration screens. For any pending requests, the Show Info icon shows the current approver and confirmation number. The confirmation number represents the number (ITEM_KEY) of the Oracle User Management Registration Workflow (UMXREGWF) workflow process handling the request.

Notification Workflows

Notification workflows enable an organization to define its own email notifications that are specific to each Role or Registration Process. Notifications include:

Oracle User Management Notification Types

Notification	Recipient
Approver notifications	Each approver.
Approval confirmation notifications	Individual for whom the request was filed.
Rejection notifications	Individual for whom the request was filed.
Identity verification notifications	Individual for whom the request was filed.

For each request that requires approval as determined by the Oracle Approval Management Engine, Oracle User Management invokes the notification workflow to request approval. Notification workflows can be written to allow approvers to review the information submitted in the registration process, make changes, and provide additional information if required.

Any changes or additional information provided can be passed back to the Oracle User Management registration engine for further processing. For example, if Oracle User Management is used to provide self service registration capability for iSP (Internet Supplier Portal), then approvers can provide additional information about site and contact restrictions for the requester. Information entered by previous approvers, including comments, are available to subsequent approvers.

Oracle User Management provides the following sample notification workflows that organizations can use directly or can copy and modify based on their requirements:

Sample Notification Workflows

Name	Item Type	Description
Oracle User Management Additional Access Request notification workflow	UMXNTWF1	Sends notifications pertaining to all requests for additional access.
Oracle User Management Notification Workflow (Account Request)	UMXNTWF2	Sends notifications pertaining to all account requests.

Self-Service and Approvals

Self-Service & Approvals Layer

Once registration processes have been configured as required, individuals can subsequently perform self-service registration tasks, such as obtaining new user accounts or requesting additional access to the system. In addition, organizations can usethe Oracle Approvals Management engine to create customized approval routing for these requests. For example, an organization may enable users to request a particularly sensitive role: however, before the user is granted the role, the organization can require that two senior members of staff, such as a manager and a vice president, must approve the request.

Oracle User Management also provides self-service features for resetting forgotten passwords, and ships with the following sample self-service registration processes:

- Employee Self-Service Registration
- Customer Self-Service Registration (external individuals)

Organizations can either use these registration processes in their existing form, or as

references for developing their own registration processes.

Access Control With Proxy Users

There are a number of business scenarios in which Oracle E-Business Suite users need to grant delegates the ability to act on their behalf (act as *proxy users* for them) when performing specific Oracle E-Business Suite functions. Traditionally, delegators have done this by giving passwords for specific applications to other users, though that method of delegating access has always been considered insecure. A delegate (the proxy user) who was given another user's passwords for certain applications could assume the identity and privileges of the delegator within those applications, and only those applications.

The integration of Oracle E-Business Suite with single sign-on (SSO) solutions accentuates the drawbacks of this all-or-nothing strategy. If a delegator grants a delegate access to his SSO password, the delegate will be able to access every SSO-enabled application to which the delegator has access, not just specific applications. The proxy user feature is designed to enable limited, auditable delegation of privileges from delegators to their delegates.

Examples of Delegation

There are a number of common scenarios where a user may need to allow another user or users to interact with Oracle E-Business Suite on the original user's behalf:

- Executives allow their assistants ongoing access to selected business applications on their behalf
- Users grant peers or subordinates limited authority for a limited duration to act on their behalf while they are out of the office
- Users grant help-desk staff or other agents limited-duration access to their Oracle E-Business Suite accounts to get help and training
- Users delegate to internal audit personnel responsible for monitoring regulatory compliance
- Several users may share a common account
- Users may need to grant access to others to increase throughput during peak business periods

The Proxy User Feature

The *proxy user* feature in Oracle E-Business Suite allows users to delegate access to specific application functionality to one or more proxy users. The delegator can grant access to specific responsibilities or workflow notification types to the proxy user,

rather than having to grant access to all functionality. This provides the flexibility needed to meet typical business scenarios.

A user with the *Security Administrator* role must configure the proxy user feature initially within the User Management responsibility.

The administrator specifies:

- *Which users can create delegates who can act on their behalf*. The administrator can give all users the privileges to delegate access to other users, or select particular roles or responsibilities whose users can delegate access. Alternatively, the administrator can assign the *Manage Proxies* role to individual users to allow those users to grant access to proxy users.

- *Which responsibilities can never be delegated*. For example, responsibilities that allow a user to change personal information or see their own salary may be deemed too sensitive to allow access by other users.

- *Which users a delegator can select as proxy users*. For example, users may only be allowed to grant access to their functionality to their own managers and direct reports, rather than any user on the system.

See: Managing Proxy Users, page 3-41 for information on how to configure and manage the proxy user feature in your installation.

Once a user has delegation privileges, setting up proxy users is straightforward. The delegator accesses the Manage Proxies menu from the Settings link or gear icon at the top of the home page or any Oracle Application Framework-based page. See: Delegating Proxy User Privileges, page 3-45.

The delegator can later track which pages were accessed by the proxy user. For more in-depth auditing, the administrator must set up Audit Trail for the specific tables of interest. An administrator with the `FND_PROXY_AUDIT` permission can review Audit Trail data for actions performed by a proxy user for any delegator.

3

Oracle User Management Setup and Administration

Setup Tasks

This section discusses the setup tasks for Oracle User Management. The implementor or system administrator sets up access control and security policies in Oracle E-Business Suite by defining roles, role inheritance hierarchies, role categories, and registration processes. These components specify the different levels of access to various application menus and data that are available to administrators.

Defining Role Categories

As part of the Oracle E-Business Suite RBAC model, Oracle User Management introduces Role Categories. Administrators can create role categories to bundle roles and responsibilities to make the process of searching for roles and responsibilities easier. In the Oracle User Management Overview section, see: Role Based Access Control (RBAC), page 2-3.

Steps

1. Log on as a user that is assigned the Security Administrator role (typically as sysadmin), select the User Management responsibility in the navigator and then click the **Role Categories** subtab.

2. Go to the editable table, click the **Update** button and then click the **Create Lookup Code** button.

3. Enter the required information in the **Create Lookup Code** fields and click the **Apply** button.

Creating and Updating Roles

In Oracle E-Business Suite, a role represents a job function that confers the privileges required to perform that job. Roles can be defined to determine what applications (responsibilities) as well as what data and functions within those applications users can access. In the Oracle User Management Overview section, see: Role Based Access Control (RBAC), page 2-3.

Steps

1. Log on as a user that is assigned the Security Administrator role (typically as sysadmin), select the User Management responsibility in the navigator and then click the **Roles & Role Inheritance** subtab.

2. Click the **Create Role** button.

3. Enter the required information to configure your role and optionally continue to configure it by accessing the following:

   - **Permissions**, page 3-3. Use this tab to assign permissions to your role.

     Delegated Administration Setup Using the Security Wizard

     Information in this section only applies to delegated administration roles in the context of the Oracle User Management application.

     - **User Administration**, page 3-9. Enables you to determine the set of users that can be managed by administrators to whom your role is assigned. The administrator can assign or revoke user accounts and roles for the users you specify here.

     - **Organization Administration**, page 3-9. Enables you to determine the external organizations that can be viewed in Oracle User Management by administrators to whom your role is assigned.

     - **Role Administration**, page 3-12. Enables you to determine which roles the administrator can assign to or revoke from the set of users specified in the User Administration section.

4. Click **Save** or **Apply** to save your changes.

5. Optionally update the role by performing the following:

   1. Locate the role you want to modify by using the **Search** fields or by expanding the appropriate nodes in the **Role Inheritance Hierarchy** menu.

   2. Click the **Update** icon and modify the role as required.

Guidelines

The **Save** button saves your changes and continues to display them in the current page. The **Apply** button saves your changes and returns to the previous page. You can optionally organize your roles using role categories during the process of creating and updating roles, otherwise they will be stored under the "Miscellaneous" role category by default. For more information, see: role categories, page 3-1. You can also define any required subordinate roles or superior roles through role inheritance hierarchies, page 3-15.

Security Wizard

The Security Wizard page lists the security wizards available to the currently logged-in user. After launching the wizard by clicking its name, the user can use it to set up the data security policies associated with the role. After completion of the wizard, the user will be returned to the Create/Update Role UI.

Assigning Permissions to Roles

You can assign permissions to a role by creating a grant that specifies the navigation menu, permission sets, and/or the data security policies that are available at runtime to the role's assignees. Menus and permission sets in turn include individual functions and permissions. In the Oracle User Management Overview section, see: Role Based Access Control (RBAC), page 2-3.

Steps

1. Log on as a user that is assigned the Security Administrator role (typically as `sysadmin`), select the User Management responsibility in the navigator and then click the **Roles & Role Inheritance** subtab.

2. In the Role Inheritance Hierarchy, access the role to which you want to assign a permission and click the **Update** icon.

3. Click the **Permissions** subtab, and then click **Create Grant** button.

4. Define the grant by entering the required information and clicking **Next**:

    1. Enter the required information to identify the grant, such as Name and Effective From date.

    2. **Security Context**. These optional parameters restrict the availability of the permissions being assigned. If you do not define the security context, then permissions are available to users in all contexts. Security contexts are also referred to as *Activation Contexts*.

        1. **Operating Unit**. In many cases, an organization consists of several different

operating units. You can limit your grant to only be active in the context of an individual operating unit.

2. **Responsibility**. Responsibilities determine the applications that can be accessed by users. You can optionally limit your grant to be available only in the context of an individual responsibility, or with all responsibilities.

3. **Data Security**. You must select a business object when you create Data Security policies. For more information, see: Oracle Application Object Library Security, page 4-1.

5. If you have defined a specific object in the preceding step, then choose the object data context for the object, also referred to as the *data scope*. Specifying the object data context provides an additional level of access granularity for the object. Choose one of the following from the Data Context menu:

   - **All Rows**. This option provides access to *all rows* for the database object. For example, if the database object is a book, creating a data security policy for all rows of the object will provide access to all books catalogued in the database.

   - **Instance**. This option provides access to an *instance* of the object. A specific instance generally corresponds to a single row in the database, and is typically identified by the primary key value for the object. For example, a data security policy for the book object could contain a unique ISBN number, to return only one book from the database.

   - **Instance Set**. This option provides access to a *related set of instances* of the object. This set is specified as a predicate on the attributes of the object. The predicate is expressed as a SQL WHERE clause, and can optionally be implemented as a VPD policy. For example, a data security policy could include an instance set for all books published in the year 2013.

6. Select the required permission set or navigation menu containing the functions (permissions) that you wish to assign to the role, by choosing an option from the LOV.

7. Review your grant information and click **Finish**.

Searching For Assigned Roles

The number of roles and responsibilities in some installations can be in the tens of thousands, or even more. Since any given user can potentially have a very large number of roles and responsibilities assigned, it can be very time-consuming to determine which roles have been assigned to which users.

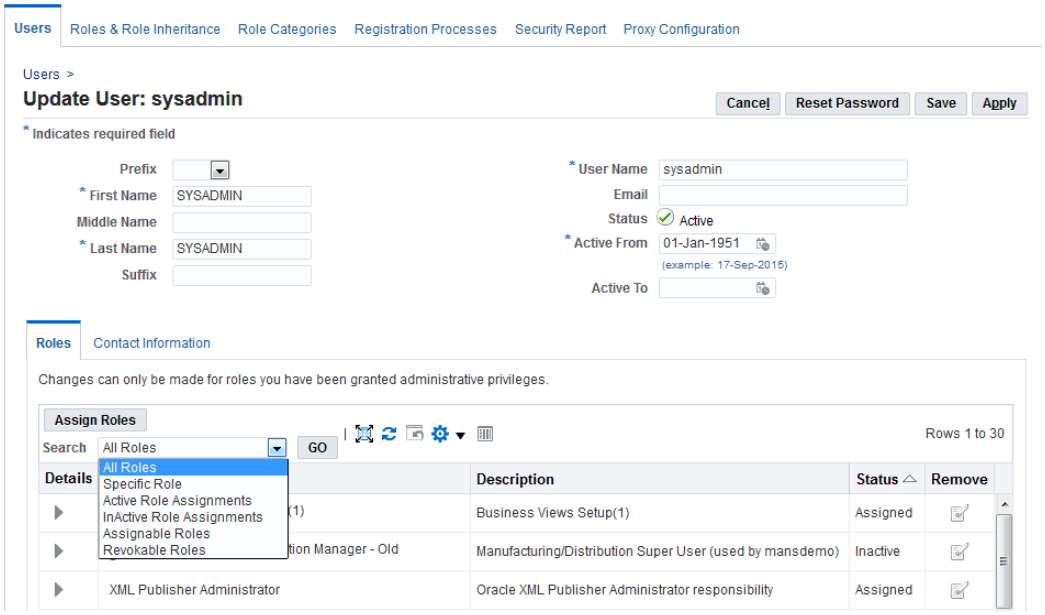
A search capability allows administrators to look for:

- **All Roles**: Find all roles assigned to the current user
- **Specific Role**: Find if a role has been assigned to an user, and quickly change the attributes associated with it.
- **Inactive Role Assignments**: Find all inactive User-Role assignments.
- **Active Role Assignments**: Find all active User-Role assignments.
- **Assignable Roles**: Find all roles for which the current logged in administrator has "Can Assign" privilege.
- **Revokable Roles**: Find all roles for which the current logged in administrator has "Can Revoke" Privilege.

Steps

1. Navigate to the User Management responsibility and then click the **Users** subtab.
2. Use the search fields to locate the required people or users.
3. Click on the **Update** icon.
4. Select any of the above specified criteria, such as "Specific Role" in the drop-down list and "Sales Manager" in the text box.
5. Click on the **Go** button.

Users Tab



Examples

- **All Roles**: If a user selects "All Roles" in the drop-down, all the roles assigned to the user will be displayed.
- **Specific Role**: If a user selects "Specific Role" from the drop-down list, another text box user appears to allow entry of a role (for example, User Management). A list of users with that role will then be displayed.
- **Inactive Role Assignments**: If a user selects "Inactive Role Assignments" from the drop-down list, all inactive User-Role assignments will be displayed.
- **Active Role Assignments**: If a user selects "Active Role Assignments" from the drop-down list, all active User-Role assignments will be displayed.
- **Assignable Roles**: If a user selects "Assignable Roles" from the drop-down list, all roles for which the current logged in administrator has "Can Assign" Privilege will be displayed.
- **Revokable Roles**: If a user selects "Revokable Roles" from the drop-down list, all roles for which the current logged in administrator has "Can Revoke" Privilege will be displayed.

Diagnostics for User-Role Assignment

UMX is heavily dependent on concurrent manager, Deferred Agents, and Background

engines. If any of these are down, the assignments do not take place or may only take place after an excessively long time.

A diagnostic feature built in the User-Role Assignment page checks that the required processes are running when an update is submitted. If they are all running, it reports how much time may be needed for the changes to be effected.

If one or more are down, the diagnostic feature displays a warning and advises which processes will need to be started in order for the changes to be made successfully. For example, you may receive a message that says: "Warning - Updates to Role data will not be visible in the application until the following processes are started: Workflow Background Engine."

Creating Instance Sets and Permission Sets

Delegated administration setup for User Administration requires the creation of instance sets and permission sets. All possible combinations of permissions are seeded as permission sets that are available from this screen. A data security object, UMX_SYS_ACCT, represents system accounts. Administrators can create instance sets against this object to specify system accounts that can be managed.

Steps

1. Log on as a user who has been assigned the Security/LSA Administrator role (typically as `sysadmin`), select the User Management responsibility in the navigator, and then click **Roles & Role Inheritance**.

2. In the role hierarchy, access the role to which you want to assign user administration privileges, and click the **Update** icon.

3. Click on the **Security Wizards** button.

4. Click on the **Run Wizard** icon for "User Management: Security Administration Setup."

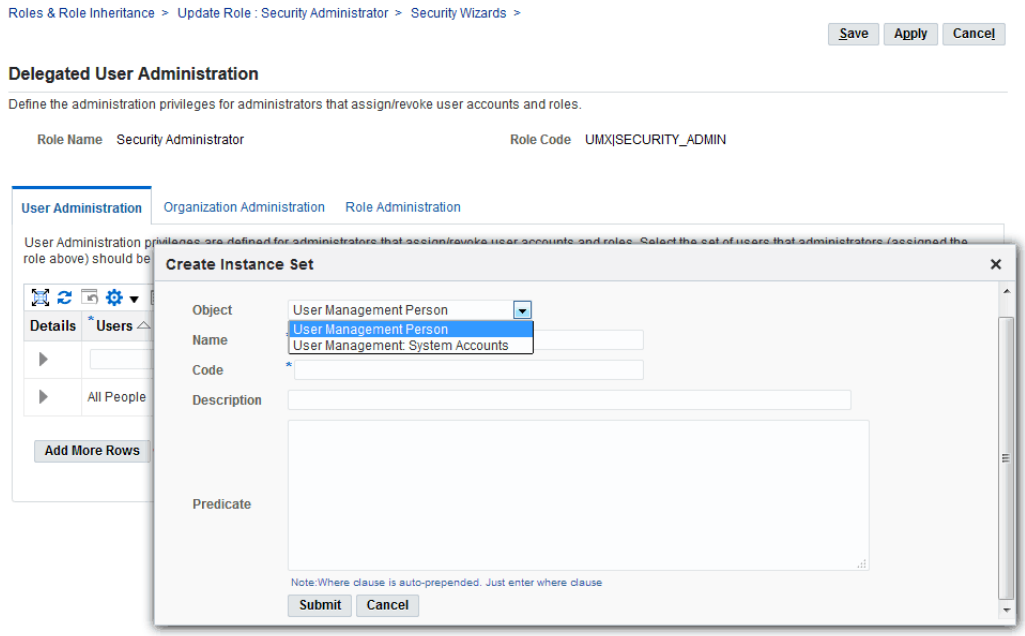
5. Click the **User Administration** tab, then click the **Add More Rows** button.

6. In the **Users** field, select the set of users that can be managed by Administrators to whom the role is assigned. The drop-down list contains various data security policies that relate to the User Management Person Object (UMX_PERSON_OBJECT) and User Management: system accounts object (UMX_SYS_ACCT). The user can now create his own policies on both these objects by clicking on the link "Create Instance Set For Users."

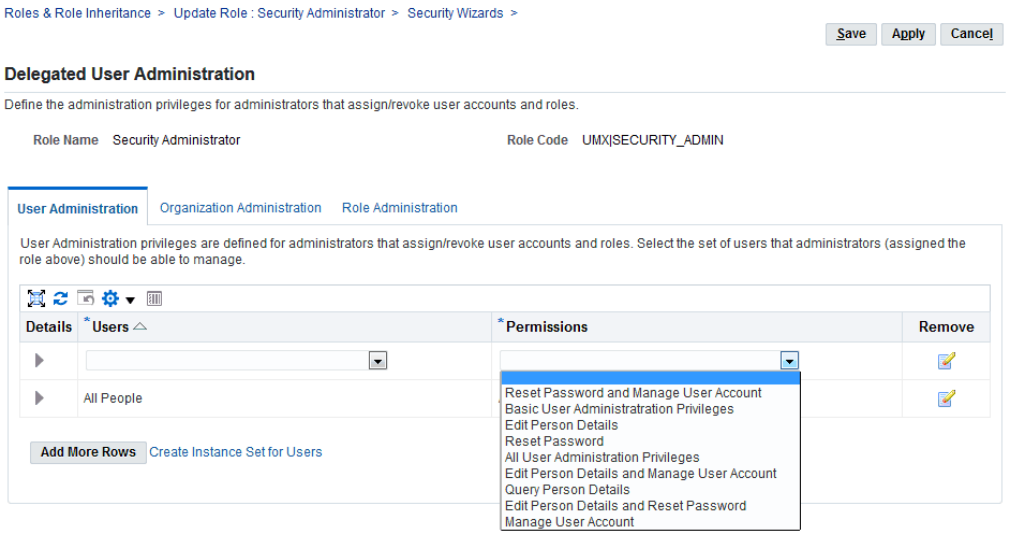
7. In the **Permissions** field, select the permissions to be associated with the delegated administration role. The Permissions drop-down list includes permission sets that contain permissions associated with the User Management Person object and User Management: system accounts object. All possible combinations of the existing

permissions have been seeded here, enabling organizations to add permission sets based on their general business needs and the level of granularity they prefer for administering users.

Create Instance Set Window



Selecting Required Permission Set (Data Security Policy)



This capability means that there is no longer any need to navigate to the Functional Administrator or Functional Developer responsibilities when creating permission sets and instance sets, so that the entire delegated administration set up should now take no more than a few minutes.

Defining Delegated Administration Privileges for Roles

Delegated Administration Privileges determine the users, roles and organization information that delegated administrators (local administrators) can manage. Each privilege is granted separately, yet the three work in conjunction to provide the complete set of abilities for the delegated administrator. In the Oracle User Management Overview section, see: Delegated Administration, page 2-6.

Defining User Administration Privileges for Roles

A local administrator must be granted User Administration Privileges to determine the users and people the local administrator can manage. Local administrators can be granted different privileges for different subsets of users. For example, a local administrator can be granted privileges only to query one set of users, and granted full privileges (including update and reset password) for another set. Local administrators cannot query users for which they do not have administration privileges.

Oracle User Management ships with the following seeded permissions for defining user administration privileges for roles:

Seeded User Administration Permissions

Function Code	Display Name	Description
UMX_OBJ_ACTIVATE_ACCT	Create, Inactivate, Reactivate User Account, Update Username	Permission for creating, inactivating, and reactivating user accounts, and updating user name. Must be granted with a data security policy on the User Management Person.
UMX_OBJ_EDIT_PERSON	Edit Person Details	Permission for editing person details. Must be granted with a data security policy on the User Management Person (UMX_PERSON_OBJECT) business object.
UMX_OBJ_PASSWD_MGMT	Reset Password	Permission to reset passwords. Must be granted with a data security policy on the User Management Person (UMX_PERSON_OBJECT) business object.
UMX_OBJ_VIEW_PERSON	Query Person Details	Permission to query person details Must be granted with a data security policy on the User Management Person (UMX_PERSON_OBJECT) business object. **Additional Information:** This is the minimum permission required by any security administrator that wishes to manage people and users in Oracle User Management.

Function Code	Display Name	Description
UMX_SYSTEM_ACCT_ADMINSTRATION	Maintain System Accounts (users not linked to a person)	Create, Inactivate, Reactivate, Reset Password for all System Accounts (defined as user accounts not associated with a person). **Additional Information:** Only grant to System Administrators.

Steps

1. Log on as a user that is assigned the Security Administrator role (typically as `sysadmin`), select the User Management responsibility in the navigator and then click the **Roles & Role Inheritance** subtab.

2. In the role hierarchy, access the role to which you want to assign user administration privileges and click the **Update** icon.

3. Click on the **Security Wizards** button.

4. Click on the **Run Wizard** icon for "User Management: Security Administration Setup."

5. Click the **User Administration** subtab and then click the **Add More Rows** button.

6. In the **Users** field, select the set of users that can be managed by Administrators to whom the role is assigned. The drop-down list contains various data security policies that pertain to the User Management Person Object (UMX_PERSON_OBJECT). Oracle User Management ships with sample data security policies for users. Organizations can use these policies or create their own. For more information, see: Defining Data Security Policies, page 3-14.

7. In the **Permissions** field, select the permissions that you wish to associate with the delegated administration role. Permissions determine the actions an administrator can perform when managing the set of users defined in the previous step. The **Permissions** drop-down list includes permission sets that contain permissions associated with the User Management Person object. Different combinations of the existing permissions can be grouped into new permission sets, enabling organizations to add permission sets based on their business needs and the level of granularity they prefer for administering users. For more information, see: Permission Sets, page 4-60.

8. Click **Save** or **Apply** to save your changes.

Guidelines

Delegated administration can provide different permissions on different subsets of users. Once you define users and permissions for a role, you can optionally view the permissions that belong to the permission set by clicking the **Show** node. You can also remove the user administration privileges for a set of users by clicking the **Remove** icon.

Defining Role Administration Privileges for Roles

Role Administration Privileges define the roles that local administrators can directly assign to and revoke from the set of users they manage.

Oracle User Management ships with the following seeded permission for defining role administration privileges for roles:

Seeded Role Administration Permission

Function Code	Display Name	Description
UMX_OBJ_ADMIN_ROLE	Assign/Revoke Role	Permission for assigning/revoking roles in the User Management application. Must be granted with a data security policy on the User Management Role (UMX_ACCESS_ROLE) business object.

Steps

1. Log on as a user that is assigned the Security Administrator role (typically as `sysadmin`), select the **User Management** responsibility in the navigator and then click the **Roles & Role Inheritance** subtab.

2. In the navigation menu, access the role for which you want to define role administration and click the **Update** icon.

3. Click on the **Security Wizards** button.

4. Click on the **Run Wizard** icon for "User Management: Security Administration Setup."

5. Click the "Role Administration" link and use the **Available Roles** fields to search for the role(s) that you want to associate with this role and which administrators can manage once they are assigned this role.

6. Select the desired role(s), move them to the Selected Roles column and click **Save** or **Apply**.

Guidelines

The **Save** button saves your changes and continues to display them in the current page. The **Apply** button saves your changes and returns to the previous page.

Defining Organization Administration Privileges for Roles

Organization Administration Privileges define the external organizations a local administrator can view in Oracle User Management. This privilege enables an administrator to search for people based on their organization, assuming the local administrator has also been granted access to view the people in that organization (User Administration Privileges). Depending on what administration account registration process has been granted, the administrator may have the ability to register new people for that organization.

Oracle User Management ships with the following seeded permission for defining organization administration privileges for roles:

Seeded Organization Administration Permission

Function Code	Display Name	Description
UMX_OBJ_VIEW_RLTNSHPS	Query/Register Organization Relationship	Permission to query/register organization relationship. Must be granted with a data security policy on the User Management Organization (UMX_ORGANIZATION_OBJECT) business object.

Steps

1. Log on as a user that is assigned the Security Administrator role (typically as `sysadmin`), select the **User Management** responsibility in the navigator and then click the **Roles & Role Inheritance** subtab.

2. In the navigation menu, access the role to which you want to define organization administration and click the **Update** icon.

3. Click on the **Security Wizards** button.

4. Click on the **Run Wizard** icon for "User Management : Security Administration Setup."

5. Click the "Organization Administration" link and then click the **Assign**

Organization Privileges button. The drop-down list contains various data security policies that pertain to the User Management Person Object (UMX_PERSON_OBJECT). Oracle User Management ships with sample data security policies for organization administration privileges. Organizations can use these policies to create their own.

6. Search for and select the appropriate organization privileges.

7. Click **Save** or **Apply** to save your changes.

Guidelines

The **Save** button saves your changes and continues to display them in the current page. The **Apply** button saves your changes and returns to the previous page.

Defining Data Security Policies

With Oracle E-Business Suite, organizations can use Data Security to manage permission assignments that control access to objects. Data Security policies can only be defined for applications that have been written to utilize the Data Security Framework. For more information, see: Overview of Data Security, page 4-18. Access to the specific object must be formed with a specified Data Security Policy (also referred to as the Data Scope or Access Policy). The Data Security Policy restricts operations so that they only can be performed on a subset of instances of the corresponding database object. For more information, see: Object Instance Sets, page 4-44.

Steps

1. Log on as a user with the Functional Developer responsibility, click the **Functional Developer** responsibility in the navigator, navigate to the **Security** tab and then click the **Objects** subtab.

2. Search for and access the object for which you want to create data security policies. For example, to locate the User Management Person business object (UMX_PERSON_OBJECT), enter "UMX%" in the **Code** field, click the **Go** button, and then click User Management Person object (UMX_PERSON_OBJECT) in the search results list. For any object for which you are creating a policy, ensure that the SQL statement returns the primary key value for that object. In this example, this is a list of person party IDs.

3. Click the **Object Instance Sets** subtab. Click the **Create Instance Set** button to create a new object instance set or click the **Update** icon to modify an existing one.

4. Enter the required information and then click the **Apply** button.

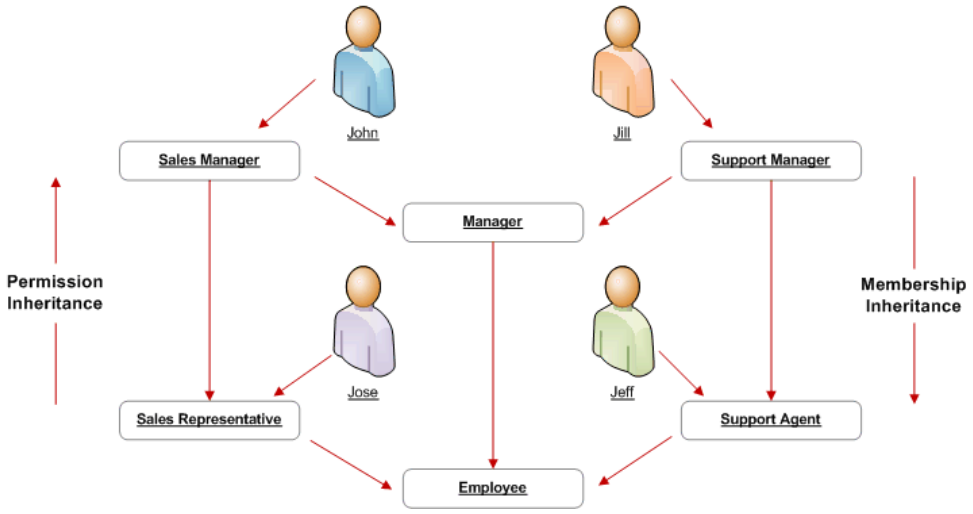
   Caution: For performance reasons, ensure that SQL predicates are tuned properly. For security reasons, ensure that they are tested and

that they return the correct result. Oracle is not responsible for the performance or correctness of data security policies defined by organizations.

Defining Role Inheritance Hierarchies

With role inheritance hierarchies, a role can contain sub roles. When a user is assigned a role, the user inherits the privileges defined for that role and for all of its sub roles. For example, the Sales Manager role can contain the Manager and Sales Rep roles, both of which in turn contain the Employee role. Any individual who is granted the Sales Manager role automatically inherits the Manager, Sales Rep and Employee roles.

Role Inheritance Hierarchies



With Role Inheritance hierarchies, roles inherit the permissions assigned to their sub roles.

Steps

1. Log on as a user that is assigned the Security Administrator role (typically as `sysadmin`), select the User Management responsibility in the navigator and then click the **Roles & Role Inheritance** subtab.

2. Locate the role for which you want to create a role inheritance hierarchy by using the Search fields or by expanding the appropriate nodes in the Role Inheritance Hierarchy menu. If you are building a role inheritance hierarchy that contains several roles, start with highest level role to which you want to add inherited subordinate roles.

3. Click the **Add Node** icon next to this role.

4. In the resulting menu, search for the role either by using the Search fields or by locating it in the Role Inheritance Hierarchy menu.

5. Select the role and then click the **Select** button or the **Quick Select** icon.

6. Repeat this process until you have added all of the required subordinate roles to their corresponding super roles. You can optionally verify the results by expanding the nodes for all super roles within your role inheritance hierarchy. You can also remove any subordinate roles by clicking the **Remove Node** icon.

Deployment Options

Organizations can use different deployment options for role inheritance hierarchies depending on their requirements.

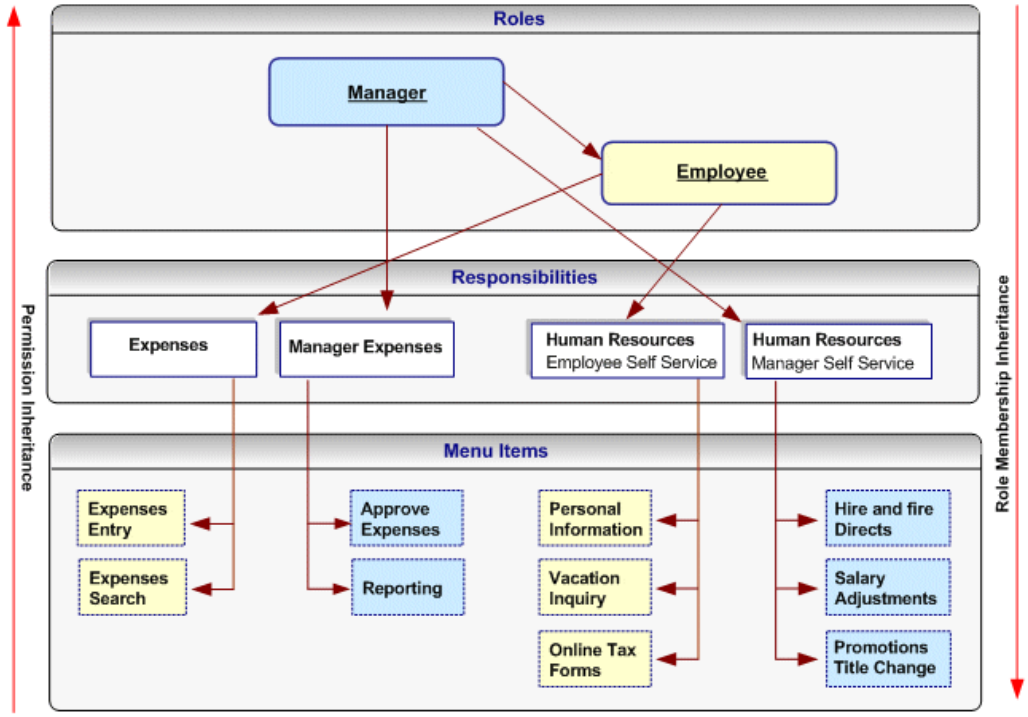
Assigning Existing Responsibilities to Roles Using Role Inheritance

Organizations that have already defined their responsibilities can utilize RBAC by creating roles and assigning their existing responsibilities to those roles. For example, an organization could create an Employee role and a Manager role, and add to these the Expenses and Human Resources responsibilities that it wishes to make available to employees and managers respectively. Then, instead of manually assigning or revoking each of these responsibilities to or from its employees, the organization can simply assign or revoke the Employee and Manager roles as required. Since the Manager role inherits the employee role, managers that are assigned the Manager role also inherit all the responsibilities and privileges associated with the Employee role.

In the following example, a Human Resource Manager inherits the Human Resources Manager Self Service responsibility through the Manager role as well as the Human Resources Employee Self Service responsibility, which the Manager role inherits from the Employee role.

> **Additional Information:** In this section, references to the Expenses and Human Resources responsibilities are used as examples only. Some applications may require organizations to create multiple responsibilities to operate with their existing security models. For more information, consult the application-specific documentation.

Assigning Existing Responsibilities to Roles Using Role Inheritance



Steps

1. Create roles representing the required job functions such as Manager and Employee.

2. Define a role inheritance hierarchy. For more information, see: Defining Role Inheritance Hierarchies, page 3-15.

3. Ensure the responsibilities are inherited by their corresponding roles.

4. Assign the roles to users as required.

Fully Utilizing RBAC and Role Inheritance to Determine Access to an Application

In older releases of Oracle E-Business Suite, access to individual functions within an application could only be defined through responsibilities, menu hierarchies, and menu exclusions. Responsibilities had the dual role of defining application navigation menus and granting permissions to the application. New responsibilities with one of the following had to be defined for each set of users with different job functions that required access to a set of pages within an application:

- A completely new menu hierarchy for each responsibility, or

- A common menu covering the superset of all functions within the application, and menu exclusion rules defined for each responsibility.

The Human Resources application, for example, typically required a minimum of two responsibilities, one for employees and one for managers.

Separating Navigation Menus and Access Control

Oracle User Management provides new alternatives for defining access to an application with RBAC and Role Inheritance, allowing organizations to separate navigation menus from access control. Responsibilities can now be defined to represent an application itself and as a result, only one responsibility may be required for each application. A menu can be tailored for each application with specific consideration to usability and end user navigation experience. Access to parts of the application (responsibility) and its corresponding menu hierarchy are instead controlled by different roles, each representing a specific job function or set of people.

Benefits

Using this mechanism for determining access control provides several benefits.

- Administration and changes can be accomplished with minimal effort:
  - A new page only has to be added to a single menu.
  - The permission to access a new page, only has to be granted once to the lowest level (subordinate role) in the role inheritance hierarchy.
  - An entirely new application (responsibility) can automatically be assigned to a set of people by simply defining it as the subordinate role of an existing role.
  - Permissions to access the various pages and functions within a new application should only be assigned at the lowest level in the role inheritance hierarchy. The permissions are then automatically inherited by all superior roles in the hierarchy.
  - Revoking access to a page, or an entire application, can be accomplished as easily as adding access.
- Improved end user experience. In the applications navigator, end users will see a list of applications to which they have access. Access to the various functions within each application is determined by the roles assigned to the end user.

Steps

> **Additional Information:** In this section, references to the Expenses and Human Resources responsibilities are used as examples only. Some applications may require organizations to create multiple responsibilities to operate with their existing security models. For more information, consult the application-specific documentation.

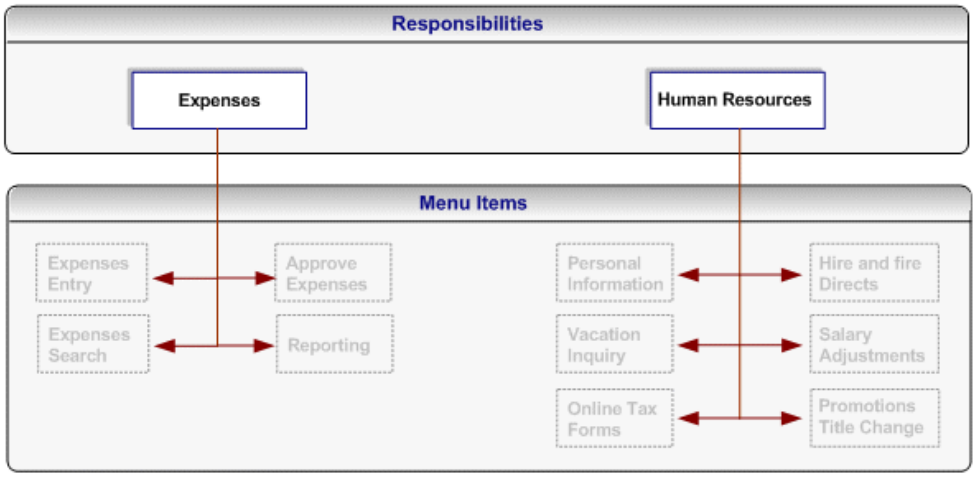
1. Define a new responsibility that will be used to represent a specific application such as Expenses or Human Resources. For more information, see: Defining a Responsibility, page 4-6.

2. Design a complete menu that includes all the menu functions within an application as well as any required submenus, and attach this menu to the new responsibility. For example, both the Expenses and Human Resources responsibilities would include all employee and manager menus. For more information, see: Defining a New Menu Structure, page 4-36.

3. Following the "principle of least privilege," all the menu options within the application (each menu item corresponds to a function/permission) should be disabled by default. To accomplish this, remove the selection from the "grant" checkbox for each menu item:

   The following figure illustrates application responsibilities (in this case, Expenses and Human Resources) with all their menus disabled:

Responsibilities Representing an Entire Application with Disabled Menus

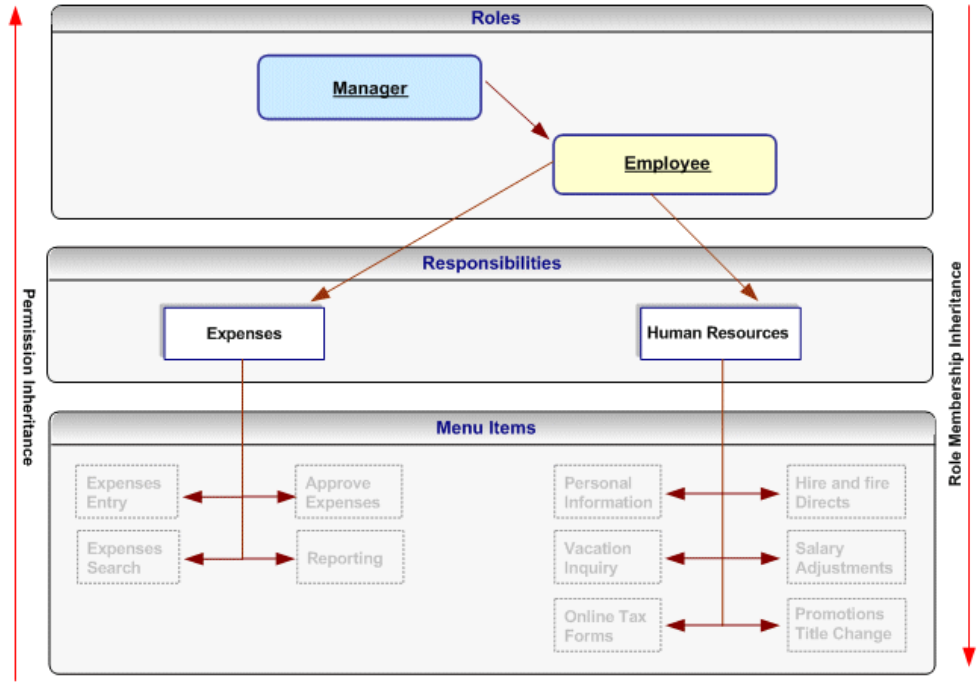


Additional Information: A user cannot access any of the menu items (functions) within the application if you assign the responsibility to the user at this stage.

4. Create roles representing the people with various job functions that require access to the application, for example, a Manager role and an Employee role. For more information, see Creating and Updating Roles, page 3-2

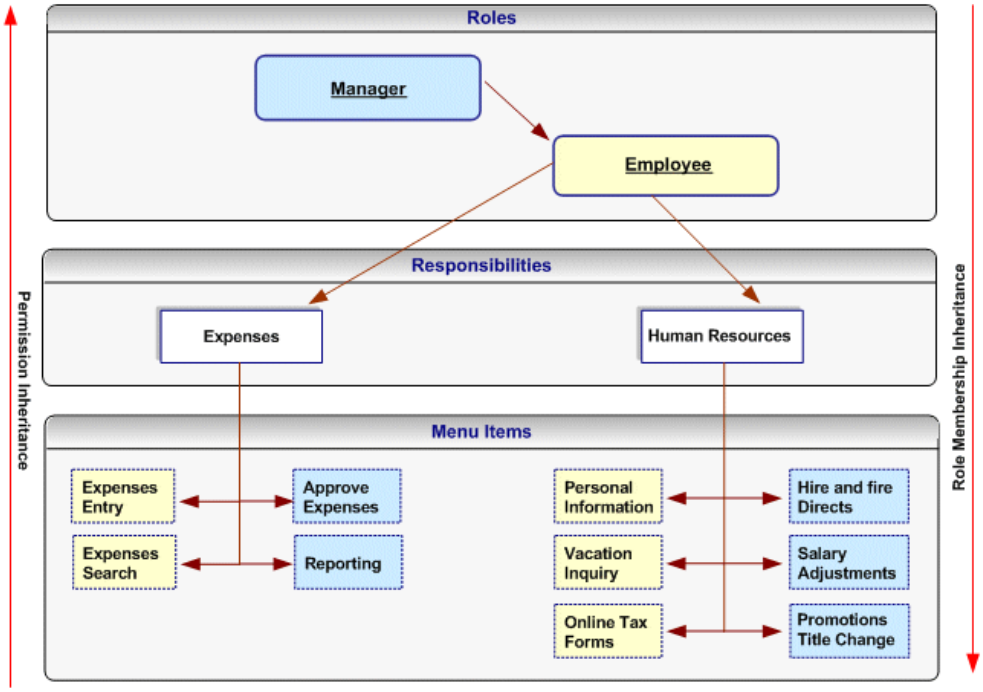
5. Define role inheritance relationships. For more information, see Defining Role Inheritance Hierarchies, page 3-15 For example, the Manager role should inherit the Employee role, and the Employee role should inherit the Expenses and Human Resources responsibilities. The following figure illustrates a role inheritance relationship in which a role inherits the responsibilities that are inherited by its subordinate role:

Role Inheritance Relationship in Which a Role Inherits the Responsibilities Inherited by its Subordinate Role



6. Assign permissions to each role. For more information, see: Assign permissions to each role, page 3-3. Each permission maps to a menu item (function) within the application (responsibility) that should be available to the users to whom the role is assigned. For example, an organization will grant the employee-related permissions from the Expenses and Human Resources responsibilities to the Employee role, and will grant the manager-related permissions for these responsibilities to the Manager role. Consequently, the manager role will have access to all the menu items within these responsibilities, but the Employee role will only have access to the Employee-related functions.

Permissions, Roles, and Inheritance



Permissions assigned to a subordinate role in the role inheritance hierarchy are automatically inherited by the superior roles. For example, if you grant the permission for accessing the Online Tax Forms page to the Employee role, anyone with the Manager role will automatically have access to this page through role inheritance. Because the Hire and Fire Directs page is only granted to the Manager role, it is not available to users that are only assigned the Employee role.

Permissions are always assigned through permission sets, which represent named sets of functions (permissions). When determining what permissions (functions/menu items) should be granted to each role, you may have to create new permission sets. For more details, see: Permission Sets, page 4-60. Menus and permission sets are stored in the same tables in the database; which means that they are interchangeable (both can be used) to assign permissions.

7. Optionally assign any additional permissions and data security policies to roles as required by each application.

Guidelines

Oracle User Management ships with the following Customer Administrator and Security Administrator roles. These roles illustrate how to setup Roles and Role Inheritance to determine user access within an application (responsibility). Both roles inherit the User Management responsibility but each role is granted different permissions and data security policies. The User Management responsibility has the grant flag removed for all functions (permissions) in the menu hierarchy. Instead, these

permissions are granted to the role depending on each role's requirements:

Role Attributes and Roles

Role Attribute	Customer Administrator	Security Administrator
Permission Sets	• User Maintenance UIs	• User Maintenance UIs • Setup screens • Maintain system accounts
User Administration	• Data security policies to manage people and user accounts for the customer administrator's own organization • Typically, the Customer Administrator can only assign or revoke a subset of roles	• Data security policies to manage all people and user accounts • The Security Administrator can assign or revoke all roles

Creating and Updating Registration Processes

Registration processes are predefined registration components that enable end users to perform some of their own registration tasks, such as requesting new accounts or requesting additional access to the system. They also provide administrators with a faster and more efficient method of creating new user accounts.

Oracle User Management provides four types of registration process:

- Self Service Account Requests
- Self-Service Requests for Additional Access
- Account Creation by Administrators
- Administrator Assisted Request for Additional Access

In the Oracle User Management Overview section, see: Provisioning Services, page 2-7.

Steps

Registration processes all use the same infrastructure and processing logic. Steps for

defining a registration process will vary depending on the type of registration process you are creating.

1. Log on as a user that is assigned the Security Administrator role (typically as `sysadmin`), select the User Management responsibility in the navigator and then click the **Registration Processes** subtab.

2. Click **Create Registration Process**.

3. Enter the required information for the Registration Process Description and click **Next**. This information specifies:

   - **Role**. The role with which you optionally associate the registration process and that is assigned to the user at the end of the registration process once the request has been processed.

   - **Type**. The type of registration process you wish to create.

   - **Registration Process Code**. The unique identifier for the registration process.

   - **Display Name**. The display name for the registration process.

   - **Description**. A description of the registration process.

   - **Application**. The application with which the registration process is classified. This can be used to help query the registration process.

   - **Active From**. The date from which the registration process is first active.

   - **Active To**. The date you can optionally specify to terminate the registration process.

4. Enter the runtime execution information for the registration process and click **Next**. This information specifies:

   - **Registration Start Page**. The first page (which is represented as a function) in the registration process that captures any additional user registration information. This is optional unless you are creating a Self Service Account Request registration process.

   - **Notification Event**. The workflow business event that invokes a workflow. The notification workflow subscribes to the event and subsequently sends notifications to the approver or to the user.

   - **Approval Transaction Type**. The set of approval routing rules that is interpreted at runtime by the Oracle Approval Management rules engine. The rules determine whether approval is required and by what set of users based on user transaction types you have defined specifically for use with Oracle User

Management.

- **Business Event Name**. Custom business event that will be raised by Oracle User Management with context information for processing.

5. Enter the eligibility information for the registration process by selecting the appropriate roles or groups from the Available Groups column and clicking **Submit** . For Self-Service Requests for Additional Access, eligibility defines the users who are able to register for the role associated with the registration process. For Account Creation by Administrators, eligibility determines what administrators can register new users through the registration process. Oracle User Management ships with the following seeded permissions for defining eligibility policies:

Seeded Permissions for Self Service Additional Access and Account Creation by Administrators Eligibility

Function Code	Display Name	Description
UMX_OBJ_ADMIN_CRTN_FLOW	Administrator Assisted Account Creation	Permission representing "Administrator Assisted Account Creation" registration processes. This must be granted as a data security policy on the Registration Process (UMX_REG_SRVC) business object.
UMX_OBJ_ROLE_ELGBLTY	Self Service Eligibility	Permission representing registration processes for additional access. Determines the set of end users that should be eligible to register for a given role/registration process. This must be granted as a data security policy on the Registration Process (UMX_REG_SRVC) business object.

6. Register subscriptions to the appropriate business events raised by Oracle User Management, and ensure that your subscription logic writes the registration data into the appropriate destination schemas.

7. Optionally update the registration process by searching for it and clicking **Update**

in the search results page.

8. Optionally set the following profile options for registration processes of type Self Service Account Request:

   - **Registration Links**. Oracle User Management provides support for displaying different registration links on the login page based upon the application tier through which the login page is accessed. Organizations can set the server level profile option, "UMX: Register Here Link - Default Registration Process" (UMX_REGISTER_HERE_REG_SRV) to specify different destinations for the registration link.

   - **Registration Parameters**. The registration link can also contain additional parameters that are not known at design time. These parameters are available at all stages of the registration process; for example, for routing approval requests. You can set the server level profile option "UMX: Register Here Link - Default Registration Parameters" (UMX_REGISTER_HERE_REGPARAMS) for this purpose. The format for setting this profile option is: "ParamName1=ParamValue1&ParamName2=ParamValue2":

   - **UI-specific Parameters**. Organizations can additionally specify parameters used to control the rendering of the registration user interface, such as the menu displayed in the registration UI. The server level profile option, "UMX: Register Here Link - Default HTML Parameters" (UMX_REGISTER_HERE_HTMLPARAMS) can be set for this purpose. The format for setting this profile option is: "ParamName1=ParamValue1&ParamName2=ParamValue2":

     Additional Information: The Apache server may need to be restarted for the changes to take effect.

Configuring the User Name Policy

The Oracle User Management registration infrastructure supports a *configurable user name policy*. This policy is used to generate a suggested user name in the sample user creation flows shipped with the application, as well as for validating the chosen user name format.

Note: Oracle User Management is supplied with a default policy that identifies users by their email address.

Seeded User Name Policies

The following table lists the seeded user name policies that are shipped with Oracle E-Business Suite.

Seeded User Name Policies

Code	Description
UMX_USERNAME_POLICY: EMAIL_ADDRESS	User name policy with email address format defined as the policy.
UMX_USERNAME_POLICY:NONE	User name policy with no restriction on user name format.

Administrators can configure either of these seeded policies. In addition to these, custom policies can also be implemented if desired.

> **Note:** For details of how to create a custom policy, see My Oracle Support Knowledge Document 399400.1, *Oracle Applications User Management (UMX) Developer's Guide*.

Configuration of user name policy is a three-stage process.

Stage 1 - Suggested User Name Generation Subscription Setup

1. Log on as a user that is assigned the Workflow Administrator Web Applications responsibility (typically `sysadmin`).
2. Go to **Workflow Administrator Web Applications** and select **Business Events**.
3. From the Business Events page, search for the Business Event with the name *oracle.apps.fnd.umx.username.generate*.
4. Click on the Subscription icon to go to the Subscriptions page.
5. For the subscription corresponding to the policy, change the status to "Enabled."

Stage 2 - Validation Event Subscription Setup

1. Log on as a user that is assigned the Workflow Administrator Web Applications responsibility (typically `sysadmin`).
2. Go to **Workflow Administrator Web Applications** and then select **Business Events**.
3. From the Business Events page, search for the Business Event with the name *oracle.apps.fnd.user.name.validate*.
4. Click on the Subscription icon to go to the Subscriptions page.

5. For the subscription corresponding to the policy, change the status to "Enabled."

Stage 3 - Profile Option Setup

1. Log on as a user that is assigned the Functional Administrator responsibility (typically `sysadmin`).
2. Navigate to **Functional Administrator**, then **Core Services**, and select **Profiles**.
3. Search with the Profile Name of UMX: User Name Policy in the Maintain Profile Options page.
4. Click on the Update icon to go to the Update Profile Option page.
5. Choose a value corresponding to the policy and click **Apply**.

Additional Requirements

- In all the three of the stages above, the values set must correspond to the same user name policy.
- The listener and JVMs must be restarted after the user name policy is changed.

Delegated Administration Tasks

The Delegated Administration layer of Access Control in Oracle E-Business Suite enables local administrators to perform a variety of specifically defined administrative tasks. Once they are assigned the appropriate roles, local administrators manage the subset of users and people to which they have access by creating, updating, or disabling accounts, granting or revoking a limited subset of their organization's roles, and changing passwords.

Maintaining People and Users

Oracle User Management enables local administrators to manage people and users in the system. People are individuals in the system who may or may not possess a user account, whereas users are individuals in the system who possess user accounts. In addition, system administrators can also manage system accounts that are not linked to people.

Typically, people and users are managed by local administrators, who can perform the following tasks:

- Register new people (optional: requires access to have been granted to the "Account Creation by Administrators" registration process)
- Create, update, or disable user accounts

- Reset passwords
- Grant users access to different parts of the system by assigning or revoking roles

Common Prerequisites

The following are prerequisites for performing any delegated administration task listed in the preceding section. Each task may have additional prerequisites:

- A role that is granted the *User Maintenance UIs* (UMX_USER_ADMIN_UI_PERMS) permission set. The role must also inherit the User Management responsibility.
- Appropriate privileges for User Administration, Role Administration, and Organization Administration.
- The Query Person Details (UMX_PERSON_OBJECT) permission for the set of people and administrator can manage.
- Optionally, the Edit Person Details (UMX_OBJECT_EDIT_PERSON) permission for the set of people that the administrator can manage.
- For system administrators, the Maintain System Accounts (UMX_SYSTEM_ACCOUNT_ADMINISTRATION) permission.

Steps

1. Navigate to the **User Management** responsibility and then click the **Users** subtab.
2. Use the search fields to locate the required people or users.
3. Manage the generated list of people or users by clicking the required icon and performing the necessary steps in the resulting window. Options for managing people and users vary depending on the permissions assigned to the administrator. Oracle User Management ships with the following basic and advanced options for maintaining people and users:
   - Query users
   - Edit personal information
   - Reset password
   - Maintain account information (create, inactivate, reactivate accounts)
   - Maintain system accounts
   - Assign or revoke roles

Creating, Inactivating, and Reactivating User Accounts

Administrators can create a user account for any person in the system who does not already possess one.

Prerequisites

To create, inactivate, and reactivate user accounts, an administrator must be assigned the following:

- Common prerequisites, as detailed in the Maintaining People and Users section, Common Prerequisites, page 3-28.
- The Create, Inactivate, Reactivate User Account (UMX_OBJ_ACTIVATE_ACCT) permission for the set of people that the administrator can manage.

By default, user names are derived from the person's email address.

Steps

1. Log in as a user with a role granting you access to the User Management responsibility, select the User Management responsibility in the navigator and click the **Users** subtab.
2. Search for the person for whom you wish to create an account and then click the **Create Account** icon next to the person's name if the account does not already exist. Your search will only generate results for the subset of users that you are eligible to manage.
3. Enter or modify the required information and click **Submit**.

Guidelines

Oracle recommends that you base user names on the person's email address.

Resetting User Passwords

Oracle User Management enables administrators to reset passwords for the set of users in the system that they manage. When the password is reset, an email message is sent to the user using the UMX Password (UMXUPWD) workflow.

Prerequisites

To reset user passwords, an administrator must be assigned the following:

- In the Maintaining People and Users section, see: Common Prerequisites, page 3-28.
- The Reset Password (UMX_OBJ_PASSWD_MGMT) permission for the users that the administrator can manage

Steps

1. Log in as a user with a role granting you access to the User Management responsibility. Select the User Management responsibility in the navigator and click the **Users** subtab.

2. Use the **Search** field to locate the user whose password you wish to change and then click the **Reset Password** icon next to the user.

3. On the Reset Password page, click **Submit**.

The person for whom you reset the password receives an email notification stating that the password has expired and must be reset the next time the user logs in. This notification is sent by the UMX Password (UMXUPWD) workflow.

Unlocking Locked User Accounts

Oracle User Management enables administrators to unlock user accounts that have been locked due to unsuccessful attempts to log in using an incorrect password.

Prerequisites

To unlock an account, an administrator must be assigned the following:

- In the Maintaining People and Users section, see: Common Prerequisites, page 3-28.

- The Reset Password (UMX_OBJ_PASSWD_MGMT) permission for the users that the administrator can manage.

Steps

1. Log in as a user with a role granting access to the User Management responsibility.

2. Select the User Management responsibility in the navigator, and click the Users subtab.

3. Use the Search field to locate the user whose account you wish to unlock. The user account is locked if the Account Status column displays a padlock icon along with status "Locked."

4. Click the "Reset Password" icon next to that user and follow the steps mentioned in the section above to reset the user's password. As a result of resetting the password, the user account will be unlocked.

Assigning Roles to or Revoking Roles from Users

Oracle User Management enables administrators to assign roles to or revoke roles from the subset of users that they manage.

Prerequisites

To assign roles to or revoke roles from users, an administrator must be assigned the following:

- Common prerequisites from the Maintaining People and Users section, Common Prerequisites, page 3-28.
- The appropriate administrative privileges for the role the administrator assigns or revokes. For more information, see: Defining Role Administration Privileges for Roles, page 3-12.

Steps

1. Log in as a user with a role granting you access to the User Management responsibility, select the User Management responsibility in the navigator, and click on the **Users** subtab.
2. Search for the person to whom you wish to assign roles or from whom you wish to revoke roles.
3. From the search results table, navigate to the User Details page by clicking on the **Update** icon next to the person's name.
4. To assign a role to the user, click the **Assign Roles** button on the User Details page and select the desired role.

   To revoke a role from the user, you must end-date the role. If the role is an inherited role, you can only remove it by removing the role from which it originates in the role inheritance hierarchy. You can view a role's inheritance hierarchy by clicking on the **Show** link next to the role.

Additional Guidelines

The administrator can only grant or revoke roles for which he has the appropriate privileges. If a registration process exists for the role, it will be invoked and the request will be handled by the Oracle User Management registration engine. If not, then the role is assigned directly. If the role is associated with a registration process for existing users and the registration process has a reference for capturing additional information, then the "Additional Information Required" link is rendered. The administrator must click on this link and provide any required additional information before the request is processed.

Fine Grained Access Control for Role Administration

Fine grained access (FGA) control for roles extends the delegated administration functionality by securing administrator operations for role administration. *Fine Grained Access for RBAC* (FGA for RBAC) , provides the functionality to support requirements of

the form "this administrator can run security wizards for some roles but not others." More specifically, FGA for RBAC allows a security administrator to set up a *limited administrator*, who can only perform restricted actions on a role.

The following privileges are available for administering roles:

- **Assign Role** - Allows an administrator to assign only a certain set of roles.
- **Revoke Role** - Allows an administrator to revoke only a certain set of roles.
- **Update Role** - Allows an administrator to update only a certain set of roles.
- **Manage Grants** - Allows an administrator to create grants on a set of roles.
- **Alter Hierarchy** - Allows an administrator to change the role hierarchies of only those roles upon which this privilege is given.
- **Run Security Wizard** - Allows an administrator to run security wizards on a certain set of roles.

The security administrator can define privileges for roles via the Role Administration tab on the Delegated Administration Screen.

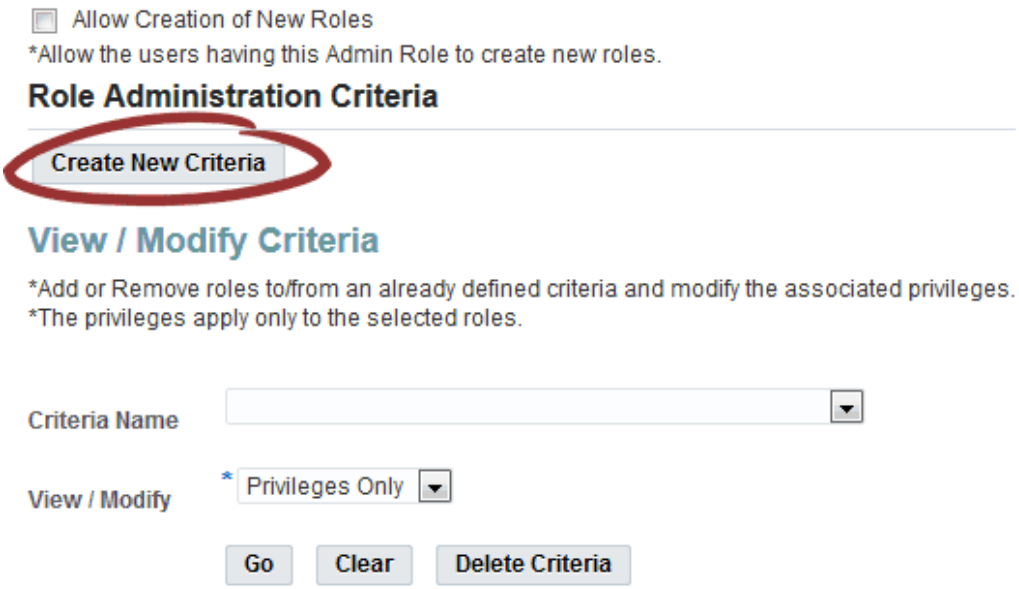
Steps

1. The Security Administrator creates a new role, such as one called Limited Security Administrator, then enables FGA on this role by running the Delegated Administration setup wizard.
2. In the setup's Role Administration tab, the Security Administrator creates a new role administration criterion, for example HRMS Role Administration. A criterion is simply a set of roles to which a set of privileges can be assigned. An administrator role can be associated with any number of criteria.
3. The Security Administrator assigns the Assign Role and Manage Grants privilege to this new criterion.

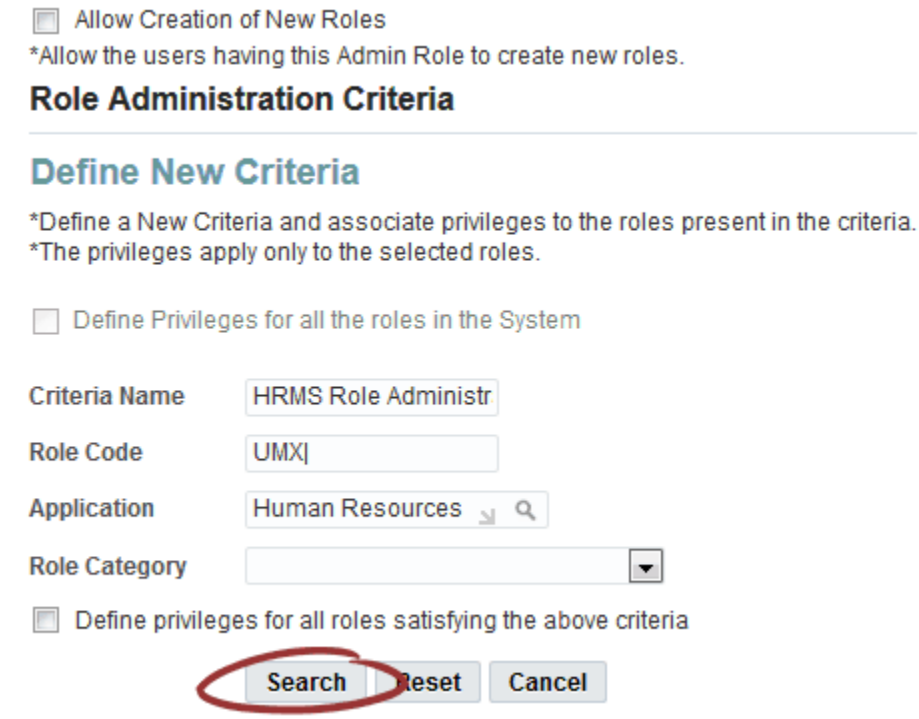
Any administrator to which the new Limited Security Administrator role is assigned will only be able to administer those roles present in the role administration criterion.

The following screenshots illustrate this process.

Create New Criteria



Define New Criteria



Select Roles and Privileges

Define New Criteria

*Define a New Criteria and associate privileges to the roles present in the criteria.
*The privileges apply only to the selected roles.

☐ Define Privileges for all the roles in the System

Criteria Name HRMS Role Administr

Role Code UMX|

Application Human Resources

Role Category

☐ Define privileges for all roles satisfying the above criteria

Search | **Reset** | **Cancel**

▶ Show Advanced Options

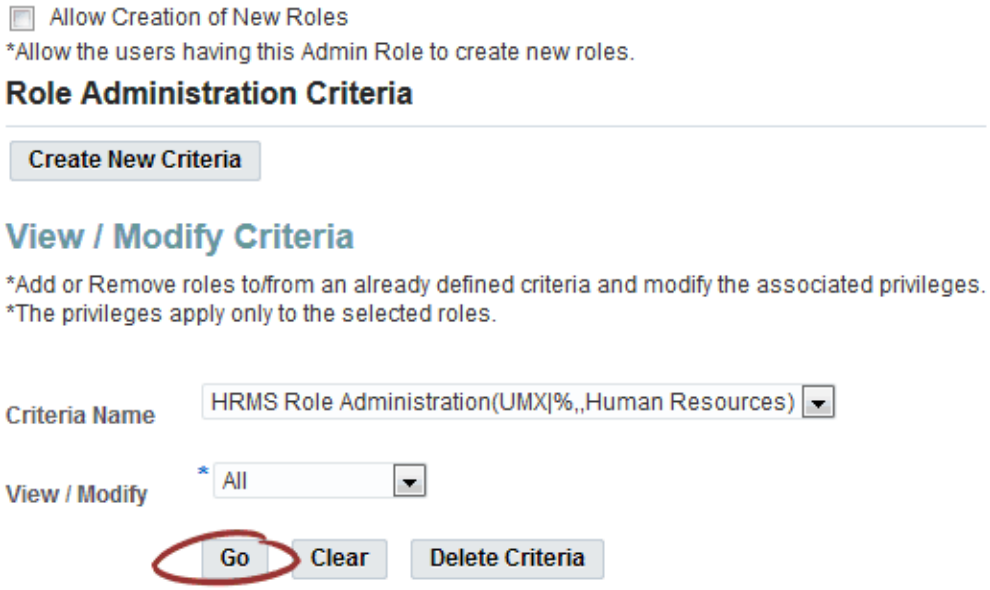
Select All | Select None

Select	Role Code	Role Name	Description
☑	UMX|AME_ADM_VIEWER	Approvals Management System Viewer	Role has access to admin dashboard with view only access.
☑	UMX|AME_APP_ADMIN	Approvals Management Administrator	Role inherits Process Owner role and System Administrator role. Can also create action type and can modify default config variables.
☐	UMX|AME_BUS_ANALYST	Approvals Management Business Analyst	Role which gives full access to business dashboard pages. Does not have Default config variable access and Action Type Create Access.
☐	UMX|AME_BUS_PROCESS_OWNER	Approvals Management Process Owner	Role can view all business dashboard view pages.
☑	UMX|AME_TTYPE_ADMIN	Approvals Management System Administrator	Role can create, update or delete transaction types. Also inherits System Viewer. Can access Exceptions log and config variables.
☐	UMX|MBL|PERSON_DIRECTORY_APP_ACCES	Access Role for Person Directory Mobile App	Access Role for Person Directory Mobile App
☐	UMX|PER_ENDECA_PEOPLE_SEARCH_ROLE	PER Endeca People Search	PER Endeca People Search

Specify Privileges for Selected Roles

☐ Update Roles ☑ Manage Grants ☐ Alter Role Hierarchy
☑ Assign Roles ☐ Revoke Roles ☐ Run Security Wizard

Update Criteria



View/Modify Criteria

Allow Creation of New Roles
*Allow the users having this Admin Role to create new roles.

Role Administration Criteria

Create New Criteria

View / Modify Criteria

*Add or Remove roles to/from an already defined criteria and modify the associated privileges.
*The privileges apply only to the selected roles.

Criteria Name: HRMS Role Administration(UMX|%,,Human Resources)

View / Modify: * All

Go | Clear | Delete Criteria

Show Advanced Options

Select All | Select None

Select	Role Code	Role Name	Description
☐	UMX|AME_BUS_ANALYST	Approvals Management Business Analyst	Role which gives full access to business dashboard pages. Does not have Default config variable access and Action Type Create Access.
☑	UMX|AME_BUS_PROCESS_OWNER	Approvals Management Process Owner	Role can view all business dashboard view pages.
☐	UMX|MBL|PERSON_DIRECTORY_APP_ACCES	Access Role for Person Directory Mobile App	Access Role for Person Directory Mobile App
☐	UMX|PER_ENDECA_PEOPLE_SEARCH_ROLE	PER Endeca People Search	PER Endeca People Search
☑	UMX|AME_ADM_VIEWER	Approvals Management System Viewer	Role has access to admin dashboard with view only access.
☑	UMX|AME_APP_ADMIN	Approvals Management Administrator	Role inherits Process Owner role and System Administrator role. Can also create action type and can modify default config variables.
☑	UMX|AME_TTYPE_ADMIN	Approvals Management System Administrator	Role can create, update or delete transaction types. Also inherits System Viewer. Can access Exceptions log and config variables.

Specify Privileges for Selected Roles

☐ Update Roles ☑ Manage Grants ☐ Alter Role Hierarchy
☑ Assign Roles ☑ Revoke Roles ☐ Run Security Wizard

Managing System Accounts

UMX formerly supported data security policies for users with a party_id in the TCA schema (HZ_PARTIES table). All such user operations were based on the "User Management Person" Object (UMX_PERSON_OBJECT). As this object was based on the HZ_PARTIES table, it could only manage users linked to a person, or (to put it another way) who had a party_id in the TCA schema. Actions such as "Query Person Details," "Reset Password," "Edit Person Details," and "Create, Inactivate, or Reactivate Account" on users were dependent on data security policies and permissions granted on the User Management Person Object (UMX_PERSON_OBJECT). Administrators therefore had to create data security policies on the User Management Person Object (UMX_PERSON_OBJECT).

This raised the question of how to administer system accounts, which lack a party_id. UMX had a permission called "Maintain System Account" Permission, which used to maintain all users who lacked party_id. Administrators with this permission could perform all operations on users who lacked a party_id. However, this did not address the issue of how to administer some sets of system accounts with restricted operations.

UMX_SYS_ACCT Object

A data security object called User Management: system accounts (UMX_SYS_ACCT) is now provided to support accounts that lack a party_id in the TCA Schema. This User Management: system accounts object is based on the database object (table) FND_USER.

Steps to use UMX_SYS_ACCT:

1. Log on as a user who has been assigned the Security Administrator role (typically as `sysadmin`), select the User Management responsibility in the navigator, and click the Roles & Role Inheritance subtab.

2. In the role hierarchy, access the role to which you want to assign user administration privileges, and click the Update icon.

3. Click **Security Wizards**.

4. Click the **Run Wizard** icon for "User Management: Security Administration Setup."

5. Click the User Administration subtab, then click on link "Create Instance Set For Users."

6. Click **Add More Rows**.

7. In the **Users** field, select the set of users who can be managed by administrators to whom the role was assigned. The drop-down list contains various data security policies that pertain to the "User Management Person" and "User Management: system accounts" objects. Select the instance set that you created in Step 5.

8. In the **Permissions** field, select the permissions that you wish to associate with the delegated administration role.

   If you want to query a user and reset his password, select "Query and Reset Password" permission set in the drop-down

9. Click Apply or Save or to save your changes.

Registering External Organization Contacts

Oracle User Management provides a sample registration process that enables administrators to register new people for their organizations. Organizations can use the sample registration process directly or reference it as an example of how to define their own administration registration processes.

Prerequisites

To register new people, an administrator must be assigned the following:

- The common prerequisites detailed in the Maintaining People and Users section, Common Prerequisites, page 3-28.
- The necessary privileges to invoke the specific administrative account creation registration processes; these are defined as part of the registration process definition.
- Organization Administration privileges for all organizations for which an administrator needs to be able to register new people.

Steps

1. Log in as a user with a role granting you access to the User Management responsibility, select the User Management responsibility in the navigator and click the **Users** subtab.
2. In the Register dropdown list, select administrative account registration process you wish to invoke, and click **Go**.
3. Enter the information required by the registration process as defined by the registration UI for the registration process, click **Submit** and then click **OK** in the resulting page.

Registering User Accounts

From the User Maintenance page under User Management, choose "User Account" from the Register list and click **Go** to register an Oracle E-Business Suite user. This user is an authorized user of Oracle E-Business Suite, and is uniquely identified by a user name.

Once defined, a new Oracle E-Business Suite user can sign on to Oracle E-Business Suite and access data through Oracle E-Business Suite windows.

The Create User Account user interface pages are similar to the Oracle Forms-based Users window.

> **Note:** If you have upgraded from a previous release of Oracle E-Business Suite, ensure that you have run the Party Merge concurrent program to update your user data. If you have not run this program, you may receive errors in querying your user data.
>
> For more information, see the Oracle Trading Community Architecture documentation.

After you have entered the information below, you can click **Submit**.

> **Note:** This user creation procedure is seeded as registration process "UMX_USER_ACCOUNT_CREATION." This registration process can

be updated with the addition of an approval process. A notification will be sent to the approver. When the approver approves, the user is created.

Click the **Assign Roles** to assign roles and update details for the user.

Account Information

Enter these fields for the user.

User Name

An application user enters this user name to sign on to Oracle E-Business Suite.

The user name should only contain characters allowed by Oracle Single Sign-On.

> **Tip:** We recommend that you define meaningful user names, such as the employee's first initial followed by their last name. Or, for a group account, you can define the application user name so as to indicate the purpose or nature of the group account.

Active From/To

Enter the date range for which this user account will be active.

The user cannot sign on to Oracle E-Business Suite before the start date or after the end date. The default for the start date is the current date. If you do not enter an end date, the user name is valid indefinitely.

You cannot delete an application user from Oracle E-Business Suite because this information helps to provide an audit trail. You can deactivate an Oracle E-Business Suite user at any time by setting the End Date to the current date.

If you wish to reactivate a user, change the End Date to a date after the current date, or clear the End Date field.

Email

Enter the email address for this user.

Fax

Enter the fax number for this user.

Password Expiration

- Days - Enter the maximum number of days between password changes. A pop-up window prompts an application user to change their password after the maximum number of days you specify has elapsed.

- Access - Enter the maximum allowed number of sign-ons to Oracle E-Business Suite allowed between password changes. A pop-up window prompts an application user to change their password after the maximum number of accesses you specify has elapsed.

  Tip: We recommend that you require all application users to make regular password changes. This reduces the likelihood of unauthorized access to Oracle E-Business Suite.

Link to a Party

Use the Person, Supplier, and Customer fields to enter the name of an employee (person), customer, or supplier contact. Enter the last name and first name, separated by a comma, of the employee, customer, or supplier who is using this application user name and password. Use the List of Values to select a valid name.

For more information on using these fields, see the Oracle Trading Community Architecture documentation.

Update User

After clicking **Assign Roles** on the Create User Account page, you can add details for roles, contact information, and securing attributes.

Roles

Click **Assign Roles** to search for existing roles and assign them to this user. Enter a justification for each role.

Contact Information

If you have chosen to link this user to a party, you can view contact information here. Note that personal information originates from the human resources system and cannot be updated here.

Securing Attributes

Securing attributes are used by some Oracle HTML-based applications to allow rows (records) of data to be visible to specified users or responsibilities based on the specific data (attribute values) contained in the row.

You may assign one or more values for any of the securing attributes assigned to the user. If a securing attribute is assigned to both a responsibility and to a user, but the user does not have a value for that securing attribute, no information is returned for that attribute.

For example, to allow a user in the ADMIN responsibility to see rows containing a CUSTOMER_ID value of 1000, assign the securing attribute of CUSTOMER_ID to the ADMIN responsibility. Then give the user a security attribute CUSTOMER_ID value of

1000.

When the user logs into the Admin responsibility, the only customer data they have access to has a CUSTOMER_ID value of 1000.

Name

Select an attribute you want used to determine which records this user can access. You can select from any of the attributes assigned to the user's responsibility.

Application

The owning application for the attribute.

Value

Enter the value for the attribute you want used to determine which records this user can access.

Reset Password

You can reset a user's password by clicking **Reset Password** and then **Submit**. The user will need to change the password upon the next login.

Alternatively, you can reset the password on the main User Maintenance page.

Managing Proxy Users

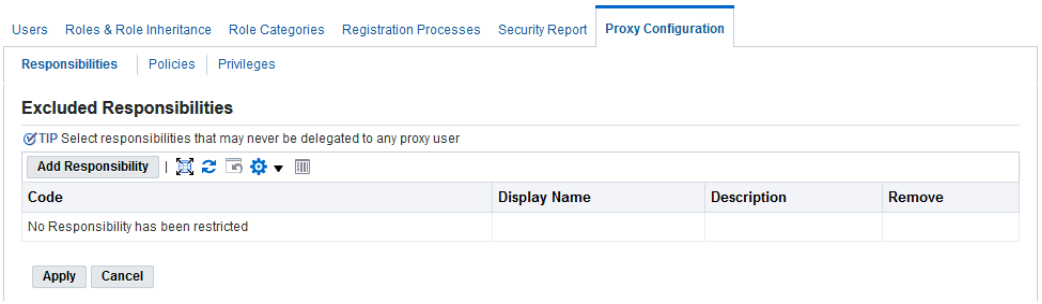
This section describes how to set up and use the proxy user feature, which allows a user to delegate some of their capabilities to another user.

> **Note:** For an introduction to this feature, see: The Proxy User Feature, page 2-16.

Defining Exclusions from Proxy User Delegation

An administrator can exclude certain responsibilities from being allowed to be delegated to proxy users. For example, you may have responsibilities such as "Employee Self-Service" where a user can change personal information and see salary and payslip information. Allowing proxy users access to other users' personal information through such responsibilities may cause privacy and legal issues. It is therefore essential to restrict delegation by proxy users as needed.

Excluded Responsibilities Page



Steps to Exclude a Responsibility from Being Delegated

1. Log in as System Administrator and navigate to **User Management** > **Proxy Configuration** > **Exclusions**.

2. Click **Add Responsibility**.

3. Select the name of the responsibility you want to exclude from delegation by users.

4. Click **Apply**.

Alternatively, if you do not want users to be able to delegate any responsibilities, administrators can disable the entire Grant Responsibility Access region of the Proxy Configuration page. To do so, set the UMX: Disable Proxy Responsibilities (UMX_PROXY_RESP_DISABLE) profile option to `Yes`. This profile option can be set only at site level. The default value is `No`.

Configuring Worklist Access

By default, when a user grants worklist access to a proxy through the Proxy Configuration page, the proxy user can view and act on notifications from the delegated item types in the worklist. However, the proxy user cannot access resources linked from a notification such as attachments, unless the associated Oracle Workflow responsibility has also been delegated to the proxy user.

Administators can optionally use the UMX: Autonomous Proxy Worklist (UMX_PROXY_WORKLIST_AUTONOMOUS) profile to enable proxy users to access linked resources from delegated notifications without having the associated Oracle Workflow responsibility explicitly delegated to them. If you set this profile option to `Yes`, then the Grant Worklist Access region in the Proxy Configuration page is disabled. Instead, a Worklist Access link appears in a tip in the Oracle E-Business Suite home page, the Oracle Workflow home page, and the worklist itself. Users can use this link to navigate to a Worklist Access page where they can grant proxy users worklist access that implicitly includes the associated Oracle Workflow responsibility access. See: Granting Worklist Access with Implicit Oracle Workflow Responsibility Access, page 3-48.

The UMX: Autonomous Proxy Worklist profile option can be set only at site level. The default value is `No`.

Making Workflow Item Types Available for Delegation

By default, the list of available workflow item types a user can delegate to a proxy displays those item types for which the user has previously received at least one notification. You can also choose to add item types that you want to appear in the lists for all users. In this way you can allow users to grant a proxy access to handle any notifications they may receive from those item types in the future.

To add an item type to the available list, define the internal name of the item type as a lookup code for the WF: Vacation Rule Item Types lookup type. See: Setting Up Notification Handling Options, *Oracle Workflow Administrator's Guide*.

Defining Proxy User Delegation Policies

An administrator can set up policies that govern which users (delegators) can select as their proxy users. Several predefined policies already exist, although you can create additional policies if needed. Creating new policies requires a thorough understanding of creating data security policies and object instance sets, therefore using predefined policies is recommended, if possible.

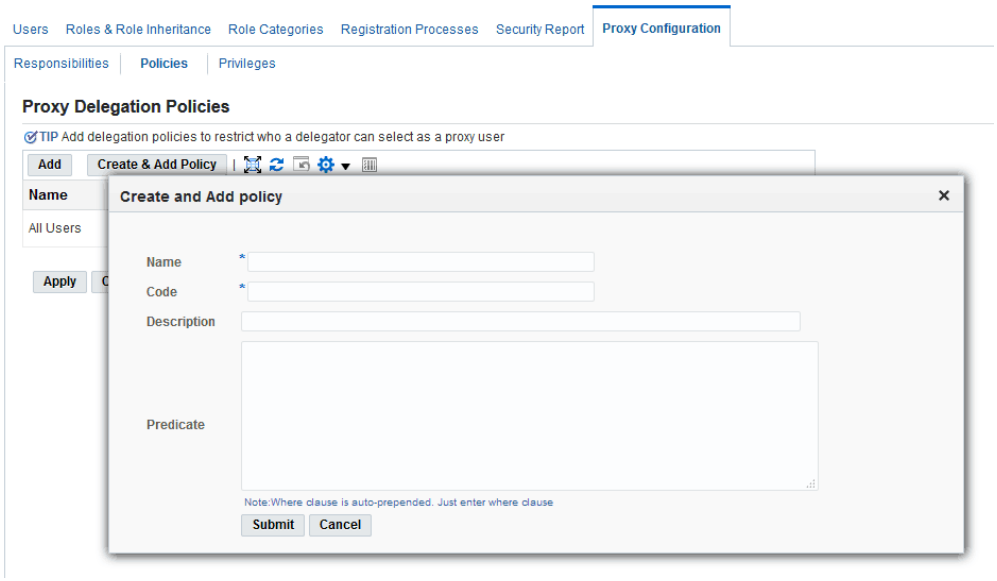
1. Log in as System Administrator and navigate to **User Management**, then **Proxy Configuration**, and select **Policies**.

2. Click **Add** to use one of the predefined policies, as described in the following table:

Proxy Delegation Policy Name	Description
All Suppliers	All suppliers belonging or visible to the organization
All Customers	All customers belonging or visible to the organization.
All Internal Users	All internal users visible to the organization.

If you want to create your own policy, click **Create & Add Policy** to create a policy specific to your organization.

Create and Add Policy Window



3. Click **Apply**.

Giving a User Delegation Privileges

There are two ways to give a user privileges to delegate to a proxy user:

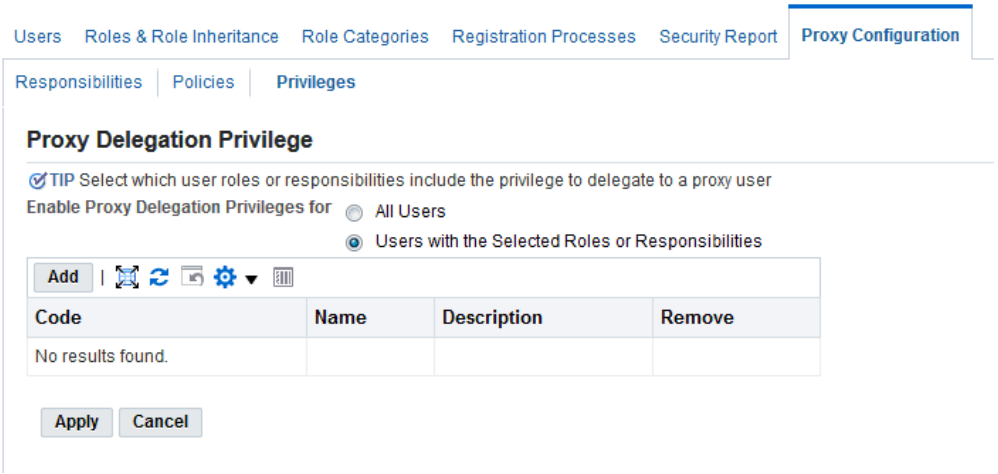
1. Use the Proxy Delegation Privilege page to give delegation privileges to all users, or users of a specific role or responsibility.

2. Use the User Details page to assign the *Manage Proxies* role to an individual user. By assigning the *Manage Proxies* role to the delegator, you make the delegator eligible to grant proxy privileges to other users to act on the delegator's behalf.

Assign Delegation Privileges to All Users or Users with a Selected Role or Responsibility

1. Log in as System Administrator and navigate to **User Management**, then **Proxy Configuration**, and select **Privileges**.

Proxy Delegation Privilege Page



2. If you want to give delegation privileges to all users, select the **All Users** option. If you want to give delegation privileges to users of a specific role or responsibility, select the **Users with the Selected Roles or Responsibilities** option, and then choose the role or responsibility you want.

3. Click **Apply**.

Assign the Manage Proxies Role to an Individual User

1. Log in as System Administrator and navigate to **User Management** and select **Users**.

2. Query the user (delegator) that you wish to have the ability to grant proxy privileges to other users: click on the Update icon of the results table to navigate to the User Details page.

3. On the User Details page, click **Assign Role**, and search for "Manage Proxies" role in the list of values.

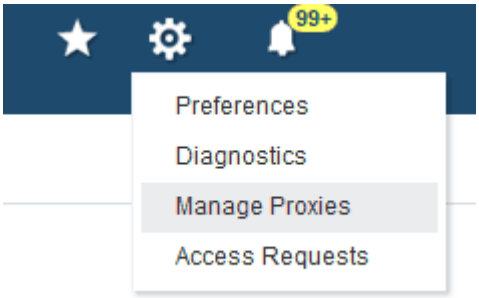
   Pick this role, supply the justification, and click **Apply**.

Delegating to a Proxy User

Once a user has delegation privileges, either by proxy user privileges configuration or by being given the Manage Proxies role directly, that user (the delegator) can then delegate other users as proxy users. For example, an employee going on vacation might want to designate her manager as a proxy user during her absence.

1. As a user with the delegation privileges, log on to Oracle E-Business Suite and click the global Settings menu.

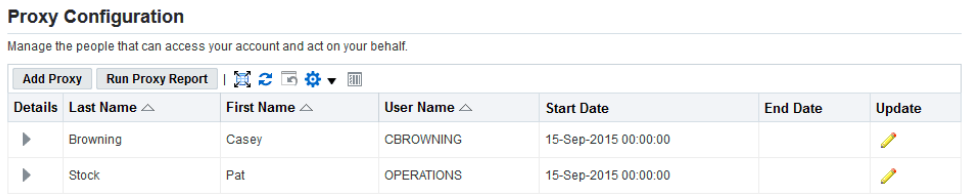
Settings Menu with Manage Proxies Menu Item Selected



2. Select **Manage Proxies** to navigate to the Proxy Configuration page, where you can see and update any existing proxies.

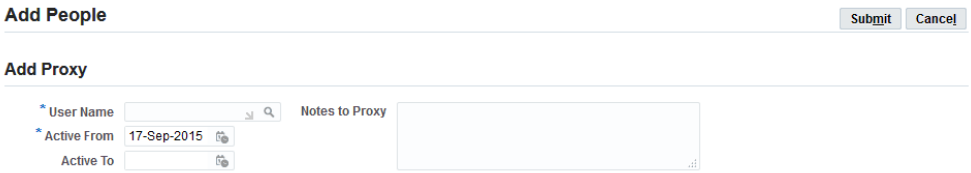
3. Click **Add Proxy** to add a new proxy user to work on your behalf.

Proxy Configuration Page



4. On the Add People page, select a user from the list of values, updating the start and end dates if required. You can also enter notes that will be displayed in the notification that your proxy user will receive to advise that he has been designated as a proxy.

Add People Page

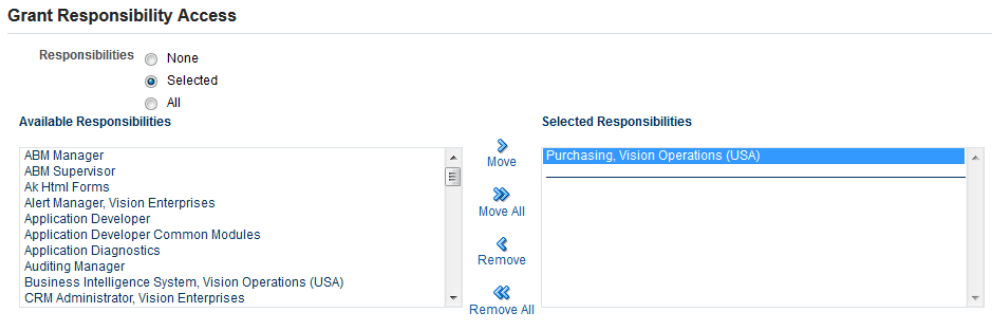


5. In the Grant Responsibility Access region, you can select None, Selected, or All responsibilities to delegate to your proxy user. If you choose the **Selected** option, you can then select any responsibilities from the Available Responsibilities list that you want your proxy user to access, and move them over to the Selected Responsibilities list. Your proxy user will see only the responsibilities you select

here when working on your behalf.

> **Note:** You may not see all of your responsibilities in the Available Responsibilities list if your administrator has excluded certain responsibilities from delegation. Additionally, if your site does not allow responsibilities to be delegated, your administrator may disable the entire Grant Responsibility Access region.

Grant Responsibility Access Region

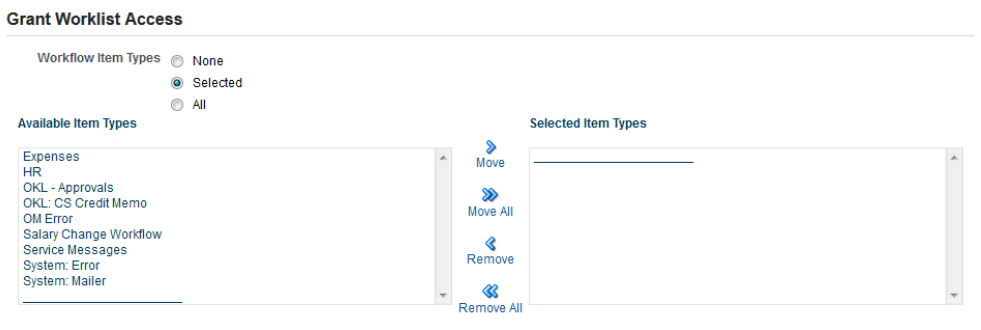


6. In the Grant Worklist Access region, you can select **None**, **Selected**, or **All** Workflow item types to delegate to your proxy user. If you choose the **Selected** option, you can then select any workflow item types from the **Available Item Types** list that you want your proxy user to access, and move them to the **Selected Item Types**. By default, the **Available Item Types** list displays those item types for which you have previously received at least one notification. Your administrator can also add item types to this list to let you grant your proxy user access to handle other notifications you may receive in the future. Your proxy user will see only the selected workflow item types when working on your behalf.

   Ensure that you also grant your proxy user the associated Oracle Workflow responsibility to allow them to access resources linked from notifications such as attachments.

   > **Note:** Your administrator may configure your site to include Oracle Workflow responsibility access implicitly when you grant worklist access. In this case, the Grant Worklist Access region in the Proxy Configuration page is disabled. Instead, use the Worklist Access page available from the Worklist Access tip link that appears in your home page or worklist. See: Granting Worklist Access with Implicit Oracle Workflow Responsibility Access, page 3-48.

Grant Worklist Access Region



7. Click **Apply** to save the changes.

8. Once the changes are saved, a notification will be sent to the user who has been granted the proxy privileges.

Granting Worklist Access with Implicit Oracle Workflow Responsibility Access

If your administrator has configured worklist access at your site to include implicit Oracle Workflow responsibility access, then you can grant worklist access through the Worklist Access page instead of the Proxy Configuration page.

1. Navigate to the Worklist Access page by navigating to the Oracle E-Business Suite home page, your Oracle Workflow home page, or your worklist, and selecting the Worklist Access tip link.

   You can review users who currently have access to your worklist. The start and end dates for each user determine the access period when the user can view and act on your worklist. The user's active or inactive status depends on whether the current date is within the access period.

   > **Note:** If a user has an e-mail address defined in Oracle E-Business Suite, you can select the link in the User Name column to send e-mail to that user.

2. To grant access to another user, choose the **Grant Worklist Access** button.

   - Select the user you want, and enter an optional description.

     > **Note:** If an administrator has restricted the user list of values, then only the values to which you have access appear in the list. See: Configuring the Oracle Workflow User List of Values, *Oracle Workflow Administrator's Guide*.

- Specify the start date when the user can begin accessing your worklist. You can optionally also specify an end date after which the user will no longer have access, or leave the end date blank to grant access indefinitely.

- Choose whether to grant the user access to notifications from all item types or only from selected item types.

  If you are granting access only to selected item types, select the item types you want in the **Available Item Types** list and move them to the **Selected Item Types** list. By default, the **Available Item Types** list displays those item types for which you have previously received at least one notification. Your workflow administrator can also add item types to this list to let you grant a user access to handle other notifications you may receive in the future. See: Setting Up Notification Handling Options, *Oracle Workflow Administrator's Guide*.

3. To update the description for a user, the start and end dates of the user's access period, or the item types to which the user has access, select the **Update** icon for that user and enter your changes.

4. To delete a user from the list, select the **Delete** icon for that user. The user will no longer have access to your worklist, even if the user's access status was previously Active.

   Note: When you delete a user, the record of the user's access no longer appears in your Worklist Access page. If you want to keep this record for reference, you can simply set the end date to end the user's access, rather than deleting the user.

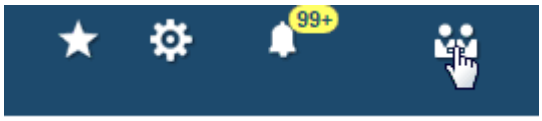
Acting as a Proxy User

If you are a user designated to act on behalf of another user (the delegator), you may initially receive a notification that you have been designated as a proxy user for the delegator, though receiving the notification is not required (and some organizations do not use Oracle Workflow).

Acting as Proxy User with Explicitly Granted Responsibility Access

1. If you are a user permitted to act on behalf of other users, a Switch User link or icon appears in the page header. Select the Switch User link or icon.

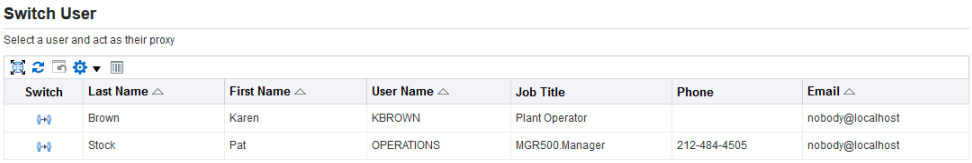
Oracle E-Business Suite Page Header Switch User Icon



2. Your own user name appears with the prefix "Logged In As" in the upper corner of the page.

3. To switch to another user (act as a delegate), choose the **Switch User** icon or link to access the Switch User page.

Switch User Page



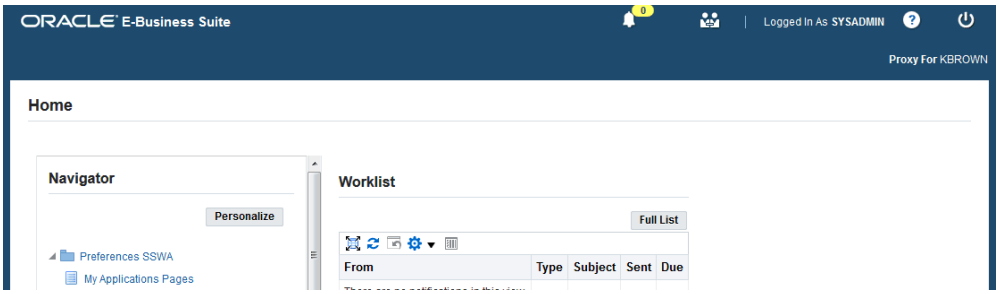
4. The Switch User page shows an alphabetical list of people who have specified that you can act on their behalf as a delegate.

5. Click on the icon in the **Switch** column to switch to Proxy Mode, where you can act on behalf of the selected user.

6. After you have selected a delegator, the application enters Proxy Mode. While you are working as a proxy user, you will see your name and the name of the user for whom you are acting as proxy. You will not see the Favorites or Settings choices in the header, nor will you see the Navigator's Top Ten List for Oracle Forms-based forms. While you are in proxy mode, the link changes from *Switch User* to *Return to Self*, though the icon remains the same.

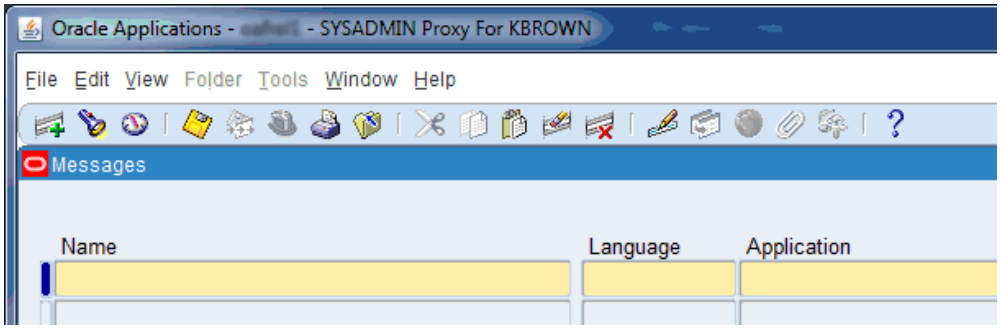
7. For most pages, a notice appears near the top of the page that says "Proxy For" with the user name of the delegator, indicating that you are acting as a proxy user for that delegator.

Proxy User Oracle E-Business Suite Home Page



If you are using a form built with Oracle Forms, a notice appears at the very top of the window showing that you are acting as a proxy user.

Proxy Oracle Forms Window



8. The user login information details reflect that you are now acting on behalf of the selected delegator.

9. Perform your tasks as the proxy.

   For more information about handling another user's workflow notifications while acting as a proxy, see: Worklist Access, *Oracle Workflow User's Guide*.

10. To exit Proxy Mode, return to the Home page and click on **Return to Self** (the **Switch User** icon).

    Note: If you are permitted to act as a proxy user for multiple delegators, you cannot switch directly from one to another. You must *Return to Self* first.

Acting as a Worklist Proxy User with Implicit Oracle Workflow Responsibility Access

1. If you have been granted access to a delegator's worklist and your site is configured to grant proxy users worklist access with implicit Oracle Workflow responsibility access, then a Switch User button appears in the Oracle E-Business Suite home page, your Oracle Workflow home page, and your worklist. To view another user's worklist, select the Switch User button.

2. The Switch User page displays the user whose worklist you were previously viewing and the list of users whose worklists you can access. Select the user whose worklist you want to view.

3. When you view another user's worklist, you can view and act on that user's notifications and access linked resources such as attachments. However, you cannot act on notifications marked as being sent from you, and you cannot define vacation rules for that user or grant access to that user's worklist to anyone else. If the other user granted you access only to selected item types, then when you view that user's worklist, the page displays only notifications that belong to those item types.

For more information about handling another user's workflow notifications while acting as a proxy, see: Worklist Access, *Oracle Workflow User's Guide*.

> **Note:** When you view another user's worklist in the Oracle E-Business Suite home page or your Oracle Workflow home page, the Full List button shows the number of open notifications to which you have access in that user's worklist, rather than your own open notifications.
>
> When you view another user's worklist in the full Advanced Worklist or Personal Worklist, the worklist page displays the name of the user to whom the worklist belongs.

Running the Proxy User Report

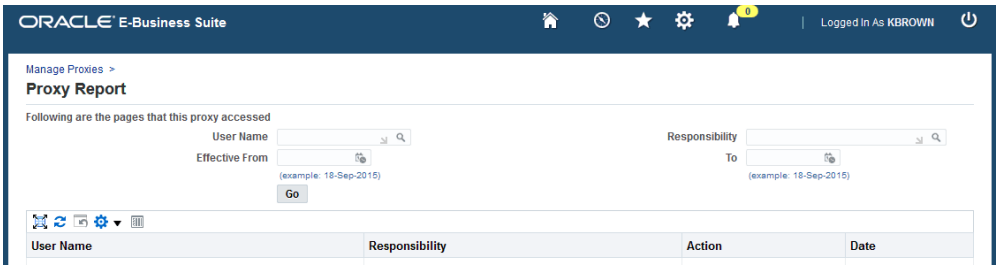
In Proxy Mode, *Page Access Tracking* (PAT) is automatically turned on to track the pages visited by the proxy user when acting on behalf of the delegator.

A concurrent program, *Page Access Tracking Data Migration*, needs to be run for the delegator to see the most recent updates in the report. The administrator must run this report.

To see a report on your proxy user's activities, perform the following steps as the delegator:

1. Under **Settings**, select the **Manage Proxies** function.
2. Select **Run Proxy Report**.
3. Specify the proxy user whose actions you want to review, the responsibility with which the proxy user performed the actions, and the start and end dates for the date range during which the proxy user performed the actions. Then run the report.

Proxy Report Page



Running the Proxy Audit Data Report

Administrators can run a report to review Audit Trail data for actions performed by a proxy user for any delegator user. To make the proxy audit data available, you must

first set up Audit Trail and run the Audit Trail Update Tables Report. See: Steps to Enable Audit Trail, page 18-2.

To run the proxy audit data report, you must log in as a user with the `FND_PROXY_AUDIT` permission. This permission is granted to the `SYSADMIN` user by default. An administrator can optionally grant it to other users.

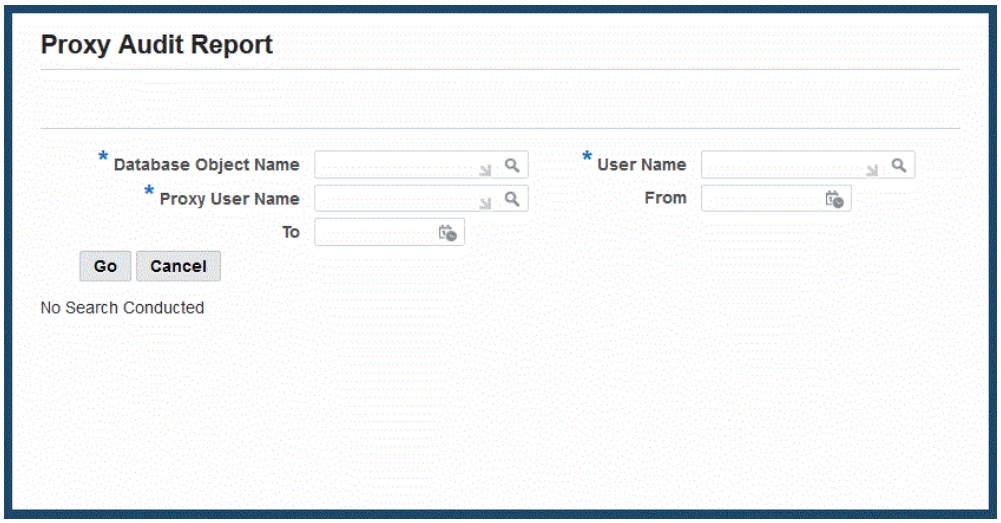
To run the proxy audit data report, perform the following steps:

1. Choose the **Settings** > **Manage Proxies** function.

2. Select **Run Proxy Audit Data Report**.

3. Specify the database object you want to review, the delegator user, and the proxy user whose actions you want to review. Optionally specify the start and end dates for the date range during which the proxy user performed the actions. Then run the report.

Proxy Audit Report Page



4. The Proxy Audit Report page submits a concurrent request for the audit report and displays the request ID. Choose the report status link to navigate to the Requests page. From this page, you can check the report status, view the report output, and optionally republish the report.

Self Service Features

Implementors and administrators can verify the successful configuration of end user functions by performing the tasks described in this section.

Self-Service Registration

Oracle User Management enables users to register for access to applications without requiring assistance from administrators. To register for application access, users must provide information in the required fields and click the **Submit** button.

Oracle User Management ships with the following sample self-service registration processes:

- Employee Self-Service Registration
- Customer Self-Service Registration (external individuals)

Organizations can use these registration processes in their existing form, or can use them as references for developing their own registration processes.

> **Important:** External users can access product functionality within Oracle E-Business Suite to perform their business tasks, including certain Oracle Workflow features such as worklist notifications and vacation rules that are available to all Oracle E-Business Suite users. These Oracle Workflow pages include user fields that by default, display all users and roles defined in Oracle E-Business Suite. Predefined responsibilities and grants are available with the July 2022 CPU patch to restrict the user and role information displayed to external users in these Oracle Workflow fields. If you define a custom security group, responsibility, or role for external users, ensure that you also define grants to secure and restrict the values displayed in the Oracle Workflow user list of values. For more information, see the following:
>
> - My Oracle Support Knowledge Document 2881609.1, *Setting Up Grants to Restrict User Access*.
> - Configuring the Oracle Workflow User List of Values, *Oracle Workflow Administrator's Guide*.
> - Your product-specific documentation.

Requesting Additional Application Access

Oracle User Management enables you to request additional access to the specific applications for which you are eligible. Application access is based on roles and to access an application you must be granted the appropriate role. Perform the following to view the roles you have been assigned and to request additional ones.

Steps

1. After logging into the system, click the **Preferences** link in the upper right corner, and click the **Access Requests** link in the sidebar menu. The Access Requests page displays the roles you have been assigned. Click the **Request Access** button to request one or more additional roles.

2. Most roles are organized according to role categories: roles that are not categorized appear under the Miscellaneous node. Select the role category that contains the role you want to request. If you do not see the required role, then either you are not eligible for the role or it has not been set up to for additional access requests.

3. Select the role or roles you require for additional access to the system, and click on the **Add to List** button. You can optionally remove roles from your list by clicking on the **Remove Roles** button.

4. When you have selected all your required roles, click on the **Next** button.

5. Enter a justification for your request and click on the **Next** button. You can remove any pending roles or check their status in the page that appears next.

Guidelines

Some roles may require you to provide additional information. In such cases, the system will prompt you for additional information before you can complete the process for requesting a role.

If the role being assigned would cause a separation of duties violation, the operation will flag this in the workflow attributes, and any approvers for the request will see the details.

Login Assistance

It is not uncommon for system administrators to have to reset a user's forgotten password, or even advise a user of the account's user (login) name. This is unproductive for both the user, who cannot do any work in the meantime, and for the administrator. In addition, a user will occasionally request the password to be reset, when it is actually the user name that has been forgotten, or vice versa. This type of occurrence leads to even more time being lost.

A new feature reduces the time spent in such administrative activities by implementing a login help mechanism that is easily accessed from the Oracle E-Business Suite Login Page. A user simply clicks on the "Login Assistance" link located below the Login and Cancel buttons.

On the screen that appears, you can either:

- Go to the Forgot Password section, enter the correct user name and then click on the **Forgot Password** button. You will then be emailed details of how to reset your

password.

- Go to the Forgot User Name section, enter the email address associated with the account, and click on the **Forgot User Name** button. The user name will then be emailed to the address specified.

For security, the relevant data is stored securely in workflow tables, and the URLs employed have both an expiration time and a single-use limitation.

The identify verification process required in previous releases of Oracle E-Business Suite is no longer needed. Instead, a link to a secure page is sent to the email address of the user name defined in the system. From this secure page, the user can change password immediately.

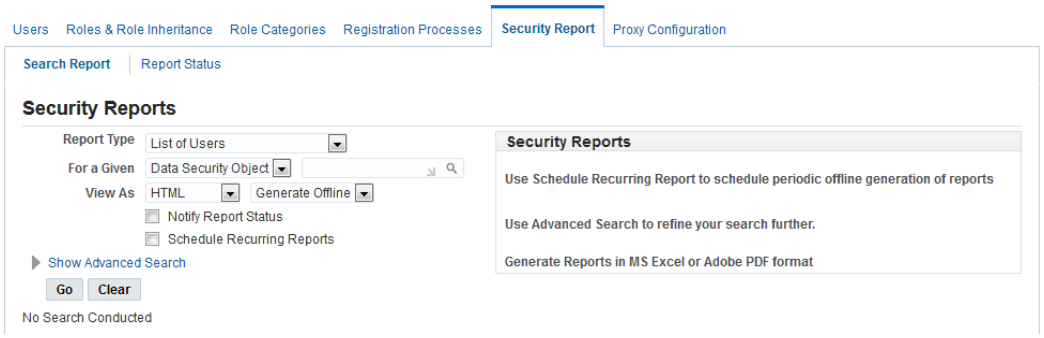
Security Reports

The Security Reports feature of UMX enables a security administrator to query the security infrastructure, identifying users who have access to specified security entities and listing the type of access those security entities grant.

Home Page

From the main page of Security Reports, the security administrator can create reports on the basis of User, Role/Responsibility, Function/Permission, or Data Security Object. A different set of reports is created for each parameter.

Security Reports Page



When creating reports, the security administrator can specify:

- The report required
- Whether the report is to be viewed online or offline
- The format of the report

In addition, the security administrator can:

- Schedule recurring reports (reports that are generated offline on a periodic basis)
- Filter conditions specific to the report, to help restrict the number of rows seen in the output

For example, a check of offline reports filed by a user might show:

Offline Report Status Page

Users | Roles & Role Inheritance | Role Categories | Registration Processes | **Security Report** | Proxy Configuration

Search Report | **Report Status**

Offline Report Status

Requests Summary Table

Refresh | Rows 1 to 12

Request ID	Name	Phase	Status	Scheduled Date	Details	Output	Republish
7553978	List of Users for Object (UMX Offline Security Reports)	Pending	Normal	17-Sep-2015 14:29:42			
7553851	List of Functions for User AMILLER (UMX Offline Security Reports)	Completed	Normal	16-Sep-2015 16:22:11			
7553842	List of Functions for User SYSADMIN (UMX Offline Security Reports)	Running	Normal	16-Sep-2015 14:52:39			
7553840	List of Users for Object (UMX Offline Security Reports)	Completed	Normal	16-Sep-2015 14:50:03			
7553825	List of Functions for User (UMX Offline Security Reports)	Completed	Normal	16-Sep-2015 12:18:18			
7553750	List of Users for Object (UMX Offline Security Reports)	Completed	Normal	15-Sep-2015 23:20:10			
7553748	List of Roles for User (UMX Offline Security Reports)	Completed	Normal	15-Sep-2015 23:14:01			
7553747	List of Roles/Responsibilities for Object (UMX Offline Security Reports)	Completed	Normal	15-Sep-2015 23:13:57			
7553746	List of Objects for User (UMX Offline Security Reports)	Completed	Normal	15-Sep-2015 23:13:49			
7553745	List of Functions for User (UMX Offline Security Reports)	Completed	Normal	15-Sep-2015 23:13:46			
7553744	List of Roles for User (UMX Offline Security Reports)	Completed	Normal	15-Sep-2015 23:13:35			
7553743	List of Users for Function (UMX Offline Security Reports)	Completed	Normal	15-Sep-2015 23:12:59			

The following sections describe some the reports that can be produced.

Listing Functions for a User

This report will display assigned functions to a given user. The main record will show:

- Function display name
- Internal name
- Function type
- Who columns

For each main record there will be a detail row that will show all the paths from which this function is available to the end user, whether it is accessible from that path, and if not, the reason and the date of assignment.

List of Functions Report

List of Functions for User AMILLER

Rows 1 to 30

Details	Display Name	Function Name	Function Type	Created By	Creation Date	Last Updated By	Last Updated Dat
▶	AMV_ADMIN	AMV_ADMIN	JSP		01-Jan-1980	ORACLE12.2.0	17-Sep-2013
◢	AMV_CATEGORIES	AMV_CATEGORIES	JSP		01-Jan-1980	ORACLE12.2.0	17-Sep-2013

Assigned Through	Accessible	Reason	Assignment Start Date	Assignment End Date
IBU_SYS_ADMIN	✗	User/Resp Start or End date is greater or less than SYSDATE	07-AUG-2001	10-NOV-2002

▶	AMV_MYCHANNELS	AMV_MYCHANNELS	JSP		01-Jan-1980	ORACLE12.2.0	17-Sep-2013
▶	AMV_PUBLISH	AMV_PUBLISH	JSP		01-Jan-1980	ORACLE12.2.0	17-Sep-2013
◢	KPI Definition	BISTARGT	FORM		17-May-1999	ORACLE12.0.0	24-Dec-2002

Assigned Through	Accessible	Reason	Assignment Start Date	Assignment End Date
PREFERENCES	✓	Through Responsibility	12-NOV-2004	

▶	Business Views Catalog Search	BIS_BV_CATALOG_SEARCH	WWL		01-Jan-1980	ORACLE12.0.0	31-Oct-2005
▶	Flexfield Form Extension	BIS_FLEXFIELD_FORM_EXTENSION	JSP		09-Sep-2002	ORACLE12.0.0	03-Apr-2006
▶	Performance Measure Region	BIS_INDICATOR_REGION	WWL		05-Aug-1999	ORACLE12.1.0	29-Aug-2005

Filter Conditions

This report has the following filters:

- **Function Type**: Zero or one function types can be selected; only those records which have this function type will be shown.
- **Include Global Granted Functions**: This filter allows or prevents information on functions assigned from global grants being added to the report.
- **Function Name/Function Display Name**: This filter accepts a wildcard for function name, and can be used to check if a given user has this function.

Listing Data Security and Business Objects for a User

The fields listed in the main table for this report are:

- **Object Name**: The internal code for the object, and a sortable column for this table.
- **Object Display Name**: The user-friendly name for the object.
- **Database Object Name**: The database object with which the object is associated.

The detailed region (Show/Hide) contains the following information:

- **Instance Type**: The type of object instance to which the user has access. Valid values for this field are:
  - Set

- Instance
- All/Global

- **Assignment Type/Assigned Through**: This field indicates the source via which the user has an access on this object. Valid values for this field are:
  - Role Grant
  - User Grant
  - Global
  - Permission set: The permission set name through which the user has access on this object, the permissions are shown as a comma separated values.

As the same object could be assigned through multiple paths, all the paths are shown here.

List of Objects Report

List of Objects for User AMILLER

Rows 1 to 30

Details	Display Name	Object Name	Database Object Name
	PROJECTS	PA_PROJECTS	PA_PROJECTS_ALL
	Parties	HZ_PARTIES	HZ_PARTIES
	JTF_TASK_RESOURCE	JTF_TASK_RESOURCE	JTF_RS_RESOURCE_EXTNS
	Persons Legislation	HR_PERSON_LEGISLATION	HR_PERSON_LEGISLATION_V
	Resources	JTF_RS_RESOURCE_EXTNS	JTF_RS_RESOURCE_EXTNS
	Resource Groups	JTF_RS_GROUPS	JTF_RS_GROUPS_B
	Resource Teams	JTF_RS_TEAMS	JTF_RS_TEAMS_B

Assigned Through	Instance Type	Menu	Permissions
GLOBAL	SET	PROJECT_GUEST_ROLE	PA_PROJ_OVERVIEW_FUNC
GLOBAL	SET	PJI_VIEW_PERFORMANCE	PJI_VIEW_PROJ_PERF,PJI_VIEW_PROJ_PERF_RN

Assigned Through	Instance Type	Menu	Permissions
GLOBAL	GLOBAL	JTF_TASK_RESOURCE_ACCESS	JTF_TASK_RESOURCE_ACCESS,CAC_TASK_RS_GROUPS_SEC,CAC_TASK_RS_EXTNS_SEC,CAC_TASK_RS_TEA

Filter Conditions

This report has the following filters:

- **Database Object Name**: This filter is used to control which objects are shown in the report.

Listing Roles and Responsibilities for a User

The fields listed in the main table for this report are:

- **Role Display Name**: The 'user friendly' name for the role.
- **Role Type**: Can be a responsibility or role.
- **Assignment Status**: Indicates whether the User-Role/Responsibility Assignment is active or not.
- **Assignment Type:** This field indicates whether the role is directly assigned to the user, inherited by the user, or both. The valid values for this column are:
  - Direct
  - Indirect
  - Both

The detailed region (Show/Hide) contains the following information:

- **Dates information**: For all roles (both direct and indirect), this region contains information about:
  - **Effective Start Date**: Date from which the user- role relationship is active.
  - **Effective End Date**: Date on which the user-role relationship ends.
  - **Role/Responsibility Start Date**
  - **Role/Responsibility End Date**
- **Justification/Comments**: This field is shown only for roles whose assignment type is 'Direct/Both'. It lists any comments added by the administrator who has assigned the role or responsibility to the user.
- **Assigning Role**: In the case of indirect assignments, this column shows the parent role through which this role was assigned to the user.

List of Roles Report

List of Roles for User AMILLER

Rows 1 to 13

Details	Display Name	Role Type	Assignment Type	Assignment Status
	iSupport Vision Custom Business User3	Responsibilities	Direct	Inactive
	Preferences SSWA	Responsibilities	Direct	Active
	iSupport Primary User	Responsibilities	Direct	Inactive
	iSupport Business User, Vision Opearations	Responsibilities	Direct	Inactive
	iSupport Vision Custom Business User1	Responsibilities	Direct	Inactive
	iSupport Site: Primary User	Responsibilities	Direct	Active

Effective Start Date	Effective End Date	Role Start Date	Role End Date	Assigned By	Justification
13-NOV-2002	09-SEP-2004	27-JUL-2001		EBUSINESS	

Filter Conditions

- **Role Name**: Used to control which roles and responsibilities are shown in the report. This filter accepts a wild card.
- **Assignment Status**: Controls whether the end user sees Active, Inactive, or All assignments.
- **Role Type**: Controls whether the end user wants to see Roles, Responsibilities, or All.
- **Assignment Type**: This filter controls whether the end user wants to see assignment types of Direct, Indirect, Both or, or All.

Listing Users With a Given Role

The fields listed in the main table for this report are:

- **User Name**
- **Assignment Status**: Whether the User to Role assignment is active or not.
- **User Status**: Whether the user is active or not.
- **Assignment Type**: Whether the role is inherited, directly assigned, or both. Valid values for this column are:
  - Direct
  - Indirect
  - Both

The detailed region (Show/Hide) contains the following information:

- **How**: This information is given only for the relationships that are indirectly inherited by the user.
  - **Parent Role Name**: Name of the Immediate Parent Role through which this role has been inherited by the user. If the role has been assigned to this user through different paths, all the parent roles from the various paths will be shown.

- **Justification**: Given only for the relationships that are directly assigned.
  - Justification is 'ASSIGNMENT_REASON' in WF_User_Role_Assignments.

List of Users of a Given Role Report

List of Users Having Role System Administrator

Rows 1 to 30

Details	User Name	Assignment Type	Assignment Status	User Status
	COMMSERSUP	Direct	Active	Active
	USER_002	Direct	Active	Inactive
	USER_006	Direct	Active	Inactive
	TBROWN	Direct	Active	Active
	Effective Start Date: 03-FEB-1999; Effective End Date: 01-JAN-9999; Justification:			
	MFG11	Direct	Inactive	Active
	BPALMER	Direct	Active	Active

Filter Conditions

- **Assignment Type**: Controls whether 'Direct', 'Indirect', 'Both' or 'All' types are shown.

- **User Status**: Displays report based on User Status, which can be specified as 'Active', 'Inactive', or 'All'.

- **Assignment Status**: Displays report based on User to Role Assignment Status, which can be specified as 'Active', 'Inactive', or 'All'.

- **User Name**: Displays report filtered by User Name.

Listing Functions That Can Be Accessed From a Given Role

This report displays assigned functions to a given user. All columns are sortable. The main record will show Function Display Name, Internal Name, Function Type, and Who columns.

List of Functions Accessed from a Given Role Report

List of Functions for Role Partner Administrator

Rows 1 to 30

Details	Function Name	Display Name	Function Type	Created By	Creation Date	Last Updated By	Last Updated Date
	CP_DELEGATED_ADMIN_SETUP	Concurrent Processing: Security Administration Setup	JSP	ORACLE12.2.0	17-Jan-2014	ORACLE12.2.0	17-Jan-2014
	FND_GRANTS_SUMMARY	Grants Summary	JSP	INITIAL SETUP	28-Aug-2002	ORACLE12.0.0	19-Jul-2006
	FND_MANAGE_PROXIES	Manage Proxies Page	WWW	INITIAL SETUP	02-Dec-2004	ORACLE12.2.0	12-Jun-2015
	ICX_CLOSE	Close	WWW	INITIAL SETUP	02-Jul-2002	ORACLE12.2.0	09-Jul-2015

Assigned Through	Accessible	Reason
UMX	✓	Through Responsibility

Filter Conditions

- **Function Name**: This filter accepts a wildcard for Function Name, and can be used to check if a given role has the functions in question.
- **Function Type**: Only those records with the specified function type will be shown.

Listing Objects for a Given Role

The fields listed in the main table for this report are:

- **Object Name**: The internal code for the object, and a sortable column for this table.
- **Object Display Name**: The user-friendly name for the object.
- **Database Object Name**: The database object with which this object is associated.

The detailed region (Show/Hide) contains the following information:

- **Instance Type**: The type of object instance to which this role gives access. Valid values for this field are:
  - Set
  - Instance
  - All/Global
- **Assignment Type/Assigned Through**: This field indicates the parent role through which this role grants access on this object.
- **Permission Set**: The name through which the user has access on this object's permissions, which are shown as comma-separated values.

As the same function or permission could be assigned through multiple paths, all the paths are shown here.

List of Objects for a Given Role Report

List of Objects for given Role Partner Administrator

Details	Display Name	Object Name	Database Object Name
▶	User Management Organization	UMX_ORGANIZATION_OBJECT	UMX_ORGANIZATION_PVT_V
◢	User Management Person	UMX_PERSON_OBJECT	UMX_PERSON_PVT_V

Assigned Through	Accessible	Instance Type	Menu	Permissions
UMX|UMX_PARTNER_ADMIN	✓	SET	UMX_OBJ_REG_ADMIN_PERMS	UMX_OBJ_VIEW_PERSON,UMX_OBJ_EDIT_PERSON
UMX|UMX_EXT_ADMIN	✓	SET	UMX_OBJ_ADV_ADMIN_PERMS	UMX_OBJ_VIEW_PERSON,UMX_OBJ_EDIT_PERSON,UMX_OBJ_PASSWD_MGMT,UMX_OBJ_

▶	Registration Process	UMX_REG_SRVC	UMX_REG_SERVICES_B

Filter Conditions

There are no applicable filter conditions.

Listing Users for a Given Function

The fields listed in the main table for this report are:

- User Name
- Who Columns

The detailed region (Show/Hide) contains the following information:

- **Accessible Through**: The Child Role/Responsibility/Grant through which the function is accessible from this role.
- **Accessibility**: Whether the function is accessible through this path.
- **Reason**: The reason the function is not accessible.

As the same function or permission could be assigned through multiple paths, all the paths are shown here.

List of Users for a Given Function Report

List of Users for Function Salary Details

Rows 1 to 30

Details	User Name	Created By	Creation Date	Last Updated By	Last Updated Date
▶	AALLEN	JPALMER	26-Jul-2001	SYSADMIN	15-May-2006
▶	AALVI	SBISHOP	20-May-2002	SYSADMIN	15-May-2006
◢	AAMBROS	UKHRMS	16-Mar-2000	SYSADMIN	15-May-2006

Accessible Through	Accessible	Reason
SSHR_V4_UK_EMPS	✓	Through Responsibility
SSHR_V4_UK_MGRS	✓	Through Responsibility

▶	AANDRADE	MXHRMS	08-Jul-2005	SYSADMIN	15-May-2006

Filter Conditions

- **User Name**: The report can be restricted on the basis of the User Name (for example, "Joe%").

Listing Roles and Responsibilities for a Given Object

The fields listed in the main table for this report are:

- Role Display Name: User Friendly Name
- Role Type: Responsibility/Role
- Who Columns

The detailed region (Show/Hide) contains the following information:

- **Instance Type of Grant**: Can be Set, All, or Instance
- **Permission Set**: Permissions granted for this role on this object

As the same role or responsibility could be assigned through multiple paths, all the paths are shown here.

List of Roles/Responsibilities for a Given Object Report

List of Roles/Responsibilities for Object User Management Person

Details	Role Name	Accessible	Grant Name	Grant Created By	Grant Creation Date	Grant Updated By	Grant Updated Date
▶	UMX|UMX_PARTNER_ADMIN	✓	User Administration privileges	ANONYMOUS	04-Aug-2004	ANONYMOUS	04-Aug-2004
◢	UMX|SECURITY_ADMIN	✓	User Administration privileges	ANONYMOUS	04-Aug-2004	ANONYMOUS	04-Aug-2004
	Instance Type	**Menu**	**Permissions**				
	SET	UMX_OBJ_ADV_ADMIN_PERMS	UMX_OBJ_VIEW_PERSON,UMX_OBJ_EDIT_PERSON,UMX_OBJ_PASSWD_MGMT,UMX_OBJ_ACTIVATE_ACCT				
▶	UMX|ARI_CUST_ADMIN	✓	User Administration privileges	ORACLE12.0.0	05-Jul-2005	ORACLE12.0.0	05-Jul-2005
▶	UMX|UMX_EXT_ADMIN	✓	User Administration privileges	ANONYMOUS	04-Aug-2004	ANONYMOUS	04-Aug-2004

Filter Conditions

- **Role Name**: The report can be filtered on the basis of Role Name.

4

Oracle Application Object Library Security

Overview of Oracle E-Business Suite Security

As System Administrator, you define Oracle E-Business Suite users, and assign one or more responsibilities to each user.

Defining Application Users

You allow a new user to sign-on to Oracle E-Business Suite by defining an *application user*. An application user has a user name and a password. You define an initial password, then the first time the application user signs on, they must enter a new (secret) password.

When you define an application user, you assign to the user one or more responsibilities.

Responsibilities Define a User's Context

A *responsibility* provides a context in which a user operates. This context can include profile option values, navigation menus, available concurrent programs, and so on.

For example, a responsibility can allow access to:

- A restricted list of windows that a user can navigate to; for example, a responsibility may allow certain Oracle Planning users to enter forecast items, but not enter master demand schedule items.
- A restricted list of functions a user can perform. For example, two responsibilities may have access to the same window, but one responsibility's window may have additional function buttons that the other responsibility's window does not have.
- Reports in a specific application; as system administrator, you can assign groups of reports to one or more responsibilities, so the responsibility a user chooses determines the reports that can be submitted.

Each user has at least one or more responsibilities, and multiple users can share the same responsibility. A system administrator can assign users any of the standard responsibilities provided with Oracle E-Business Suite, or create new custom responsibilities if required.

HRMS Security

The Human Resources Management Systems (HRMS) products have an additional feature using Security Groups. For more information, see: *Customizing, Reporting, and System Administration in Oracle HRMS*.

Related Topics

Defining a Responsibility, page 4-6

Defining Request Security, page 4-7

Overview of Function Security, page 4-11

Form Functions, page 4-31

Responsibilities, page 4-22

Users Window, page 4-26

Enterprise Command Center Security

Oracle Enterprise Command Center Framework provides an additional script to set up responsibilities and grants for product-specific Enterprise Command Centers. You run this script as part of your initial installation of Oracle Enterprise Command Center Framework. If you later change your RBAC setup, such as by creating new custom responsibilities, then you should rerun the script to update the Enterprise Command Center setup. See My Oracle Support Knowledge Document 2495053.1, *Installing Oracle Enterprise Command Center Framework, Release 12.2*.

Oracle E-Business Suite User Passwords

The following are features related to passwords for end users of Oracle E-Business Suite.

Passwords can be defined in the Users Window; see: Users Window, page 4-26 for more information on setting user passwords.

Case Sensitivity in Oracle E-Business Suite User Passwords

Oracle E-Business Suite user passwords can optionally be treated as case sensitive, depending on the setting you choose for the site-level profile option *Signon Password Case*.

The two available settings are:

- **Sensitive** - Passwords are stored and compared as they are, with the password case preserved. During comparison, if the entered password does not match the decrypted version, then an error message is displayed. With Release 12, this option is the default behavior. All newly created or changed passwords are treated as case sensitive.

  > **Note:** Users who have not changed their passwords since the installation of Release 12 are not affected until they do change their passwords.

  A password expiration utility is available if the System Administrator requires that all users convert to case sensitive passwords upon the next login. This utility expires all passwords in FND_USER, including that of `SYSADMIN` and default Vision accounts and can be run as a SQL script (`$FND_TOP/sql/AFCPEXPIRE.sql`) or as a concurrent program (FNDCPEXPIRE_SQLPLUS).

- **Insensitive (or not set)** - Passwords are treated as case insensitive. In Insensitive mode, passwords are stored and compared in uppercase, similar to that in earlier releases. The entered password and the decrypted password are converted to uppercase prior to comparison.

If you want to preserve case insensitivity in passwords, such as retain the behavior from previous releases, ensure that Signon Password Case value is either set to "Insensitive" or not set at all.

There are no upgrade or data migration issues with this new feature. The profile option affects only how new passwords are stored. Existing passwords are tested using the policy in effect when they were created.

Non-Reversible Hash Password Scheme

For enhanced security of passwords, you can use the FNDCPASS utility to migrate local Oracle E-Business Suite user passwords from their current encryption scheme to a non-reversible hash that makes them non-recoverable.

For information on how to use FNDCPASS to migrate to non-reversible hash passwords, and information on FNDCPASS and the related AFPASSWD utilities in general, see: Oracle E-Business Suite Password Management, *Oracle E-Business Suite Maintenance Guide*.

Restriction on the GUEST User Password

The `GUEST` user password cannot include the special character "`#`."

Super User Feature for Password Profile Override

The Super User Feature for Password Profile Override feature provides the ability to

have a "Super User" whose password profile values, if set, override the site-level profile values when the Super User creates new users or updates passwords for existing users.

For this feature, the Super User is defined as one whose password profile values, if set, overrides the Site values and other password profile values when the Super User creates passwords for new users. This feature will override the following password profiles when creating a new user and/or changing an existing user password:

- Signon Password Case (SIGNON_PASSWORD_CASE)
- Signon Password Length (SIGNON_PASSWORD_LENGTH)
- Signon Password Hard to Guess (SIGNON_PASSWORD_HARD_TO_GUESS)
- Signon Password Custom (SIGNON_PASSWORD_CUSTOM) (This profile option specifies the full name of the class containing custom password validation logic.)

The profile SIGNON_PASSWORD_NO_REUSE will be overridden only when changing the password value of an existing user.

Here is an example of a business case for this feature: Say you have set the SIGNON_PASSWORD_HARD_TO_GUESS profile to 'Yes' at the Site level. Also say you have a requirement to create users whose initial passwords match their Insurance Policy Numbers. However, an insurance policy number can have repetitive digits (for example, '33'), and the repetitive numbers violate the rule specified by the profile SIGNON_PASSWORD_HARD_TO_GUESS. To overcome this conflict, this "Super User" feature can be enabled to create a Super User and the profile value for SIGNON_PASSWORD_HARD_TO_GUESS can be set to 'No' at the User level for this Super User. Now the Super User can create a new user having the password as "Insurance Policy Number" because the Super User's profile value overrides the site-level value. Note that whenever a new user gets created, the profile value is retrieved from the "Site" as the call is to fnd_profile.value_specific() API.

Note that the values which are used from the Super User setup are only temporary. Upon initial logon, each user must change the password as expected. When users sign on for the first time and change their passwords, the system enforces the password policies set at the Site- or User- level and not those of the Super User.

To enable this feature, you make a user a Super User by granting the permission 'OVERRIDE_PASSWORD_POLICY_PERM' must be granted to this user. This permission should only be granted by a system administrator who has a "Functional Administrator" responsibility.

1. Navigate to the Functional Administrator responsibility, then Permission Sets.
2. Create a permission set having the permission 'OVERRIDE_PASSWORD_POLICY_PERM'.
3. Create a grant on this permission set and assign this grant to the user.

Now, the Super User feature is activated. To deactivate this feature, end-date the grant or delete the grant.

> **Important:** This feature should only be activated if there is an appropriate business need and if the issue can be resolved only by this feature, because the impact of this implementation can be enormous.

Guest User Account

Credentials (user name and password) for the Guest user are stored in a secure repository that was specifically designed to store sensitive data such as credentials, certificates and keys. Oracle E-Business Suite products can read Guest user information from this repository using standard APIs.

> **Note:** Prior to Release 12.1, such items were stored in a FND profile option, GUEST_USER_PWD. This profile option did not offer the advanced security features now employed, and is no longer supported.

The only way to change the Guest user password is to update the context variable `s_guest_pass` and run AutoConfig, which runs the AdminAppServer utility. See: Using AutoConfig Tools for System Configuration, *Oracle E-Business Suite Setup Guide* and AdminAppServer Utility, *Oracle E-Business Suite Setup Guide*.

User Session Limits

Using the following profile options you can specify limits on user sessions.

ICX: Session Timeout

Use this profile option to enforce an inactivity time-out. If a user performs no Oracle E-Business Suite operation for a time period longer than the time-out value (specified in minutes), the user's session is disabled. The user is provided an opportunity to re-authenticate and re-enable a timed-out session. If re-authentication is successful, the session is re-enabled and no work is lost. Otherwise, Oracle E-Business Suite exits without saving pending work.

If this profile option is set to 0 or NULL, then user sessions will never time out due to inactivity.

ICX: Limit time

Use this profile option to specify the absolute maximum length of time (in hours) of any user session, active or inactive.

Defining a Responsibility

When you define a responsibility, you assign to it some or all of the components described below.

Menu (Required)

A menu is a hierarchical arrangement of application functions (forms). In the definition of a responsibility, the specified menu defines what is displayed in the navigator. The specified menu does not necessarily define the functions that can be accessed by the responsibility, which are granted. See: Overview of Function Security, page 4-11.

Data Group (Required)

A data group defines the mapping between Oracle E-Business Suite products and ORACLE database IDs. A data group determines which Oracle database accounts a responsibility's forms, concurrent programs, and reports connect to. See: Defining Data Groups, *Oracle E-Business Suite Setup Guide*.

> **Important:** Oracle Application Framework functionality does not support data groups. You should not define any custom data groups.

For almost all cases, you should accept the default value in defining a responsibility.

Function and Menu Exclusions (Optional)

A responsibility may optionally have function and menu exclusion rules associated with it to restrict the application functionality enabled for that responsibility. See: Overview of Function Security, page 4-11.

Additional Notes About Responsibilities

Predefined Responsibilities

All Oracle E-Business Suite products are installed with predefined responsibilities. Consult the reference guide for your Oracle E-Business Suite product for the names of those predefined responsibilities.

Additionally, instances of the major components that help define a responsibility (data groups, request security groups, menus, and functions) are predefined for Oracle E-Business Suite. You should not define any custom data groups.

Responsibilities and Request Security Groups

> **Note:** The Request Security Groups feature is for backward compatibility only.

When a request group is assigned to a responsibility, it becomes a *request security group*.

From a standard submission form, such as the Submit Requests form, the choice of concurrent programs and request sets to run are those in the user's responsibility's request security group.

If you do not include the Submit Requests form on the menu for a responsibility, then you do not need to assign a request security group to the responsibility.

Responsibilities and Function Security

Oracle E-Business Suite architecture may aggregate several related business functions into a single form. Parts of an application's functionality may be identified as individual Oracle E-Business Suite functions, which can then be secured (that is, included or excluded from a responsibility).

See: Overview of Function Security, page 4-11

Defining Request Security

You can control user access to requests and request sets using request security groups or Role-Based Access Control (RBAC). Beyond this short introduction, request groups and request security groups are discussed in greater detail, as part of a broader range of topics not necessarily limited to application security, in *Oracle E-Business Suite Setup Guide*.

Using Request Security Groups

You can use request security groups to specify the reports, request sets, and concurrent programs that your users can run from a standard submission form, such as the Submit Requests form.

Define a request group using the Request Groups form. Using the Responsibilities form, you assign the request group to a responsibility. The request group is then referred to as a *request security group*. See: Request Security Groups, *Oracle E-Business Suite Setup Guide* .

You can define a request group to contain single requests, request sets, or all the requests and request sets in an application.

If you choose to include all the requests and requests sets in an application, the user has automatic access to any new requests and request sets (without owners) in the future.

A request security group can contain requests and request sets from different

applications. If you want to define request security groups that own requests from different applications, refer to the discussion on Data Groups. See: Defining Data Groups, *Oracle E-Business Suite Setup Guide*.

> **Note:** A *request security group* or *request group* is not the same as a *security group*.

Individual Requests and Request Sets

Reports or concurrent programs which are not included in a request security group on an individual basis, but do belong to a request set included in a request security group, have the following privileges:

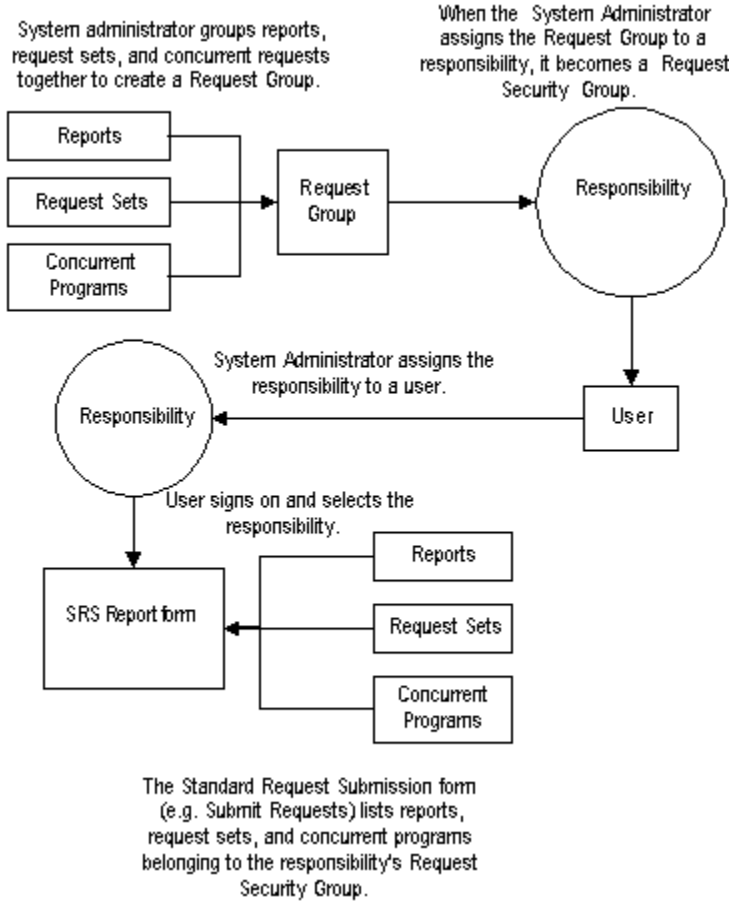
- Users can, however, run request sets that contain requests that are not in their request security group, if the request set is in their request security group.

If you assign a request set, but not the requests in the set, to a request security group, the user:

- Can edit the request set by deleting requests from it or adding other requests to it, only if the user is the assigned owner of the request set.
- Cannot edit request information in the request set definition.
- Cannot stop specific requests in the set from running.

The Request Security Groups figure below illustrates the relationship between a request security group, application user, and a responsibility.

Responsibilities, Request Groups, and Request Security Groups



Request Security Using RBAC

By using RBAC, administrators have more granular control in granting submission privileges to users. In short, administrators can assign individual programs/sets, all programs/sets in a request group, programs/sets belonging to one or more applications, and so on, either to the user directly or to a role that can then be assigned to one or more users.

If applications are included in the request groups, all programs/requests sets that are created in these applications will also be automatically included. Note that request submission applies to both programs and request sets.

See: Controlling Access to Concurrent Programs using Role-Based Access Control (RBAC), *Oracle E-Business Suite Setup Guide*.

Related Topics

Overview of Oracle E-Business Suite Security, page 4-1

Defining a Responsibility, page 4-6

Form Functions, page 4-31

Menus, page 4-36

Responsibilities, page 4-22

Users, page 4-26

Request Sets and Owners, *Oracle E-Business Suite Setup Guide*

Oracle Applications Manager Security Tests

You can manage Oracle E-Business Suite Diagnostics tests across environments from the Oracle Applications Manager Dashboard.

The two key tests accessible from the OAM Security tab are:

- Best Practices: Database Security Tests
- Best Practices: Oracle E-Business Suite Security Tests

Overview of Security Groups in Oracle HRMS

Security groups, used exclusively by Oracle HRMS, allow data to be partitioned in a single installation. A single installation can use a particular set of configuration data, but store data for multiple clients, where the data is partitioned by security groups. A user with a responsibility assignment of one security group can only access data within that security group.

A security group represents a distinct client or business entity. Data that must be distinct for each client in an installation is partitioned by security group. All other data is shared across all security groups.

For Oracle Application Object Library, the data items that are "striped" by security groups are responsibility assignments, lookups, and concurrent programs.

Security is maintained at the level of responsibility/security group pairs. That is, users are assigned specific responsibilities within each security group. When signing on to Oracle E-Business Suite, a user, if assigned more than one responsibility, will be asked to choose a responsibility and security group pair. Partitioned data accessed through security group sensitive views will show only data assigned to the current security group.

Use the Enable Security Groups profile option to enable this feature.

Defining Security Groups

Every installation will have a single "Standard" security group seeded in. If no other security groups are created, this single group will be hidden from users when they sign

on.

In the Users form, you assign a security group when you assign a responsibility.

For more information, see: *Configuring, Reporting and System Administration in Oracle HRMS.*

Overview of Function Security

Function security is the mechanism by which user access to applications functionality is controlled.

Function security can be considered as "global data security," in that it grants access to a function regardless of the current row of data.

Oracle E-Business Suite architecture aggregates several related business functions into a single form. Because all users should not have access to every business function in a form, Oracle E-Business Suite provides the ability to identify pieces of applications logic as *functions*. When part of an application's functionality is identified as a function, it can be secured (that is, included or excluded from a responsibility).

Application developers register functions when they develop forms. A system administrator administers function security by creating responsibilities that include or exclude particular functions.

Terms

Function

A function is a part of an application's functionality that is registered under a unique name for the purpose of assigning it to, or excluding it from, a responsibility.

There are two types of function: *executable functions* (originally called form functions), and *non-executable functions* (originally called subfunctions).

Executable Function

Executable functions have the unique property that you may navigate to them using the Navigate window.

Non-Executable Function

A non-executable function is a securable subset of a form's functionality: in other words, a function executed from within a form.

A developer can write a form to test the availability of a particular non-executable function, and then take some action based on whether the non-executable function is available in the current responsibility.

Non-executable functions are frequently associated with buttons or other graphical

elements on forms. For example, when a non-executable function is enabled, the corresponding button is enabled.

However, a non-executable function may be tested and executed at any time during a form's operation, and it need not have an explicit user interface impact. For example, if a non-executable function corresponds to a form procedure not associated with a graphical element, its availability is not obvious to the form's user.

Menu

A menu is a hierarchical arrangement of functions and menus of functions. Each responsibility has a menu assigned to it. Menus can map to permission sets.

Menu Entry

A menu entry is a menu component that identifies a function or a menu of functions. In some cases, both a function and a menu of functions correspond to the same menu entry. For example, both a form and its menu of subfunctions can occupy the same menu entry.

Responsibility

A responsibility defines an application user's current privileges while working with Oracle E-Business Suite. When an application user signs on, they select a responsibility that grants certain privileges, specifically:

- The functions that the user may access. Functions are determined by the menu assigned to the responsibility.
- The concurrent programs, such as reports, that the user may run.
- The application database accounts that forms, concurrent programs, and reports connect to.

Related Topics

How Function Security Works, page 4-14

Form Functions, page 4-31

Forms and Subfunctions , page 4-12

Functions, Menus, and the Navigate Window, page 4-13

Overview of Oracle E-Business Suite Security, page 4-1

Implementing Function Security, page 4-16

Executable Functions vs. Non-executable Functions

An executable function, as a whole, including all of its program logic, is always

designated as a function. Subsets of a form's program logic can optionally be designated as subfunctions if there is a need to secure those subsets.

For example, suppose that an executable function such as a form contains three windows. The entire form is designated as a function that can be secured (included or excluded from a responsibility). Each of the form's three windows can be also be designated as non-executable functions, which means they can be individually secured. Thus, while different responsibilities may include this form, certain of the form's windows may not be accessible from each of those responsibilities, depending on how function security rules are applied.

Related Topics

Overview of Function Security, page 4-11

Functions, Menus, and the Navigate Window, page 4-13

How Function Security Works, page 4-14

Functions, Menus, and the Navigate Window

Executable functions are selected using the Navigate window. The arrangement of form names in the Navigate window is defined by the menu structure assigned to the current responsibility.

The following types of menu entries are not displayed by the Navigate window:

- Non-executable functions
- Menus without Entries
- Menu Entries without a Prompt

If none of the entries on a menu are displayed by the Navigate window, the menu itself is not displayed.

Menu Entries with a Submenu and Functions

If a menu entry has both a submenu and a function defined on the same line, then the behavior depends on whether or not the function is executable. If it is executable, then the submenu on the same line is treated as content to be rendered by the function. The submenu will not appear on a navigation tree, but will be available in function security tests (FND_FUNCTION.TEST calls). If the function is not executable, then it is treated as a "tag" for enforcing exclusion rules, and the submenu on the same line is displayed in the navigation tree.

A function is considered executable if it can be run directly from the current running user interface. For example, an Oracle E-Business Suite form using Oracle Forms is an executable function from within Oracle Forms, but not within the Self Service applications.

How Function Security Works

Registering Functions

- Developers can require parts of their Oracle Forms code to look up a unique *function name*, and then take some action based on whether the function is available in the current responsibility. Function names are unique.

- Developers can register functions. They can also register parameters that pass values to a function. For example, a form may support data entry only when a function parameter is passed to it.

> **Warning:** In general, you should not modify names, parameters, or other material features of predefined functions for Oracle E-Business Suite products. The few exceptions are documented in the relevant manuals or product notes.

Excluding Functions

Each Oracle E-Business Suite product is delivered with one or more predefined menu hierarchies. System Administrators can assign a predefined menu hierarchy to a responsibility. To tailor a responsibility, System Administrators exclude functions or menus of functions from that responsibility using exclusion rules.

> **Note:** The ability to exclude functions is to be used for backward compatibility only. Menu exclusions do not apply to grants.

Read-Only Forms for a Responsibility or User

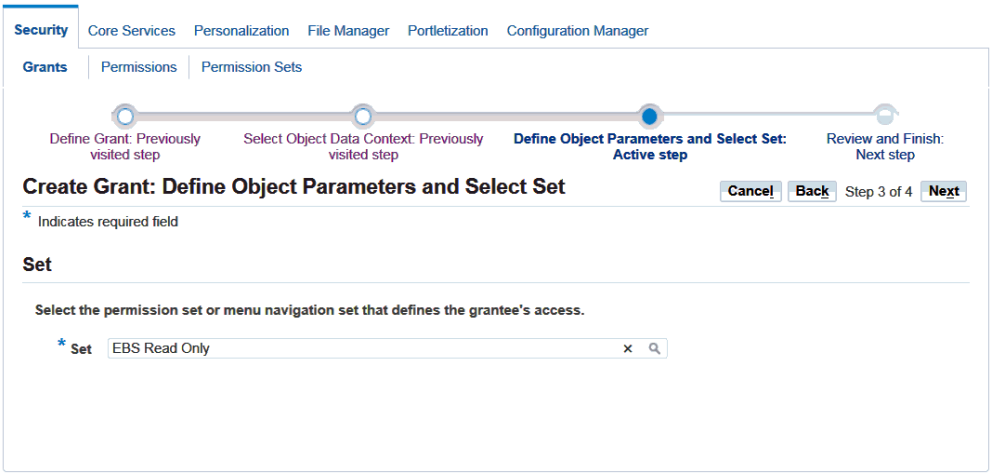
An application developer can define a form to be opened in query-only, or read-only, mode by using the QUERY_ONLY=YES string as a parameter for the function calling the form. Beginning with Release 12.2.6, an administrator can create a grant to set a form as read-only on the responsibility level, user level, or for an organization or a group of users. This can be done by granting the 'EBS Read Only' permission set to grantees.

Using the Functional Administrator responsibility, navigate to the **Grants** > **Create Grant** page.

1. On the Define Grant page, select the desired grantee type and grantee.

2. On the Define Object Parameters and Select Set page, select the permission set 'EBS Read Only' and assign it to your grantee(s).

Create Grant: Defined Object Parameters and Select Set Screen



3. Save your grant.

For more information on query-only forms, see Using Form Functions, *Oracle E-Business Suite Developer's Guide*.

Available Functions for a User

Functions are available to a user through responsibilities (as well as grants).

When a user first selects or changes their responsibility, a list of functions obtained from the responsibility's menu structure is cached in memory.

Functions a System Administrator has excluded from the current responsibility are marked as unavailable.

Executable functions in the function hierarchy (such as the menu hierarchy) are displayed in the Navigate window. Available non-executable functions are accessed by working with the application's forms.

Related Topics

Overview of Function Security, page 4-11

Overview of Data Security, page 4-18

Forms and Subfunctions , page 4-12

Overview of Oracle E-Business Suite Security, page 4-1

Form Functions, page 4-31

Implementing Function Security

Securing Functions Using New Menus

Use the Menus form to define menus pointing to functions that you want to make available to a user.

- Use forms and their associated menus of non-executable functions to define new menus.

The new menu can be then granted to a user.

Defining a New Menu Structure

When defining a new menu structure:

- Create a logical, hierarchical listing of functions. This allows for easy exclusion of functions when customizing the menu structure for different responsibilities.
- Create a logical, hierarchical menu that guides users to their application forms and pages.

Tasks for Defining a Custom Menu Structure

- Determine the application functionality required for different job responsibilities.
- Identify predefined menus, forms, and form subfunctions to use as entries when defining a new menu. Understand predefined menus by printing Menu Reports using the Submit Requests window.

  Tip: To simplify your work, use predefined menus for your menu entries. You can exclude individual functions after a menu structure is assigned to a responsibility.

- Plan your menu structure. Sketch out your menu designs.
- Define the lowest-level menus first. A menu must be defined before it can be selected as an entry on another menu.
- Assign menus and functions to higher-level menus.
- Assign menus and functions to a top-level menu (root menu).
- Document your menu structure by printing a Menu Report.

Warning: Always start with a blank Menus form (blank screen). See Notes About Defining Menus, below.

Notes About Defining Menus

Define Menus for Fast and Easy Keyboard Use

- Design menu prompts with unique first letters, so typing the first letter automatically selects the form or menu.
- Design the sequence of menu prompts with the most frequently used functions first (such as lower sequence numbers).

Menu Compilation

The Compile Security (FNDSCMPI) concurrent program is used to compile menus so that the system can more quickly check if a particular function is available to a particular responsibility/menu.

You should compile your menus after you make changes to your menu data. A request for this concurrent program is automatically submitted after you make changes using the Menus form.

Related Topics

Menus Window, page 4-36

Compile Security Concurrent Program, page 4-62

Preserving Custom Menus Across Upgrades

Preserve custom menus during upgrades of Oracle E-Business Suite by using unique names for your custom menus. For example, you can start the menu's name with the application short name of a custom application. Define a custom application named *Custom General Ledger*, whose application short name is XXCGL. Define your custom menu names to start with XXCGL, for example, XXCGL_MY_MENU.

Remember that the Oracle E-Business Suite standard menus may be overwritten with upgrade versions. Therefore, if you attached your custom menu as a submenu to one of the preseeded Oracle E-Business Suite menus, recreate the attachment to it following an upgrade. An alternative is to attach a standard Oracle E-Business Suite menu as a submenu to your custom menu; the link from your custom menu to the standard menu should survive the upgrade.

Related Topics

Overview of Oracle E-Business Suite Security, page 4-1

Overview of Function Security, page 4-11

Implementing Function Security, page 4-16

Form Functions, page 4-31

Function Security Reports, page 4-62

Overview of Data Security

Data Security allows administrators to control user access to specific data, as well as what functions users can apply to that data.

Function security can be considered "global" data security, in that access to a function is granted regardless of the data.

Concepts and Definitions

Objects

Data Security uses the concept of an Object to define the data records that are secured.

Object

Data security permissions are managed on objects. Business entities such as Projects and Users are examples of objects. Only a securable business-level concept should be registered as an object.

An object definition includes the business name of the object and identifies the main table and primary key columns used to access the object.

Object Instance

An object instance is a specific example of an object, such as Project Number 123 or User JDOE. An object instance generally corresponds to a row in the database. An instance is identified by a set of one or more primary key values as defined by the object.

In addition, "All Rows" for an object indicates all data rows of the object.

Object Instance Set

An object instance set is a group of related object instances within an object. A set is specified as a predicate on the keys or attributes of an object, expressed as a SQL "WHERE clause." All instances that satisfy the predicate are considered members of the object instance set. For example:

```
STATUS = 'ACTIVE'
```

could determine a set of object instances with the "Active" status.

The specific instances in the set can vary over time as object instance attributes change, or as new object instances are created.

An example is:

```
OWNER = FND_GLOBAL.USER_ID
```

The predicate can also be parameterized, so that the logic can define instance sets as a function of one or more input parameters. An example is:

```
COLOR = :PARAM1
```

Object instance sets are also called "data instance sets."

Users and Groups

Users and groups are both roles that you can use in Role-Based Access Control. User and role information is stored in the Oracle Workflow directory service. For more information, see: Setting Up an Oracle Workflow Directory Service, *Oracle Workflow Administrator's Guide*.

Privileges given to users and groups determine their access to secured objects.

The data security system allows you to assign privileges to groups of users instead of assigning privileges to each user individually.

Users

Users are individuals who have access to software applications at a particular enterprise.

A user must have a unique name and should map one-to-one with an individual human or system. "Group" accounts are not correct uses of the user entity.

Groups

Users can belong to Groups. The grouping can come from position or organization relationships modeled in applications such as Oracle Human Resources. Alternatively, ad-hoc groups can be created explicitly for security purposes. A group is sometimes referred to as a role.

Functions and Permissions

A function or a permission is the smallest unit of securable product functionality. You can register function definitions with the security system to represent actions that can be performed on an object or on the system in general. Granting a function to a set of users gives them permission to perform that function, and so a function may also be referred to as a permission.

There are two broad categories of functions and permissions:

- An *executable function/permission* can be invoked from a generic navigator user

interface. An executable function definition must contain all information necessary to launch the function; often this includes the form name or URL plus parameters.

- An *abstract function/permission* does not refer to a specific piece of code, but represents permission to perform a higher-level business action. The code that implements an abstract function calls the function security system to test whether the abstract function is granted. The system only allows the action if the abstract function is granted.

Examples of these are a particular JSP page (executable) and View Person (abstract).

Functions and permissions can either be at the system level or be sensitive to a data context.

Navigation Menus and Permission Sets

Functions and permissions are grouped into related sets so that administration of these functions can be performed in higher-level business terms.

Functions and permissions are bundled into named sets, which can be defined for two purposes: as navigation menus and/or permission sets. Each set can also contain other sets.

Menus are defined for navigation purposes and group UI pages into functional areas. Users access menus by selecting responsibilities. Each menu item maps to a permission which optionally may be granted to the user as part of the menu/responsibility assignment. Menu items that are not granted as part of the menu/responsibility assignment will not be rendered unless the user is granted the permission separately.

Permission sets are granted to users or roles independently of menus/responsibilities. Permission sets are granted to users in order to enable menu items and other operations (functions) that should not be available to all users assigned a given menu/responsibility. Permission sets are granted to users or roles through permission assignments (grants).

Grants

A *grant* authorizes a particular role to perform a specified action or actions (set of functions) on a specified object instance (or object instance set).

Note that where you are creating a data security policy for an object by creating a grant, you need to include that object in your grant definition. Other than in this specific type of case, you do not need to specify an object in your definition.

Security Context

Security context refers to the context of the data in which the user is working. For example, data context could be the organization or responsibility with which the user is logged in.

Implementation of Data Security

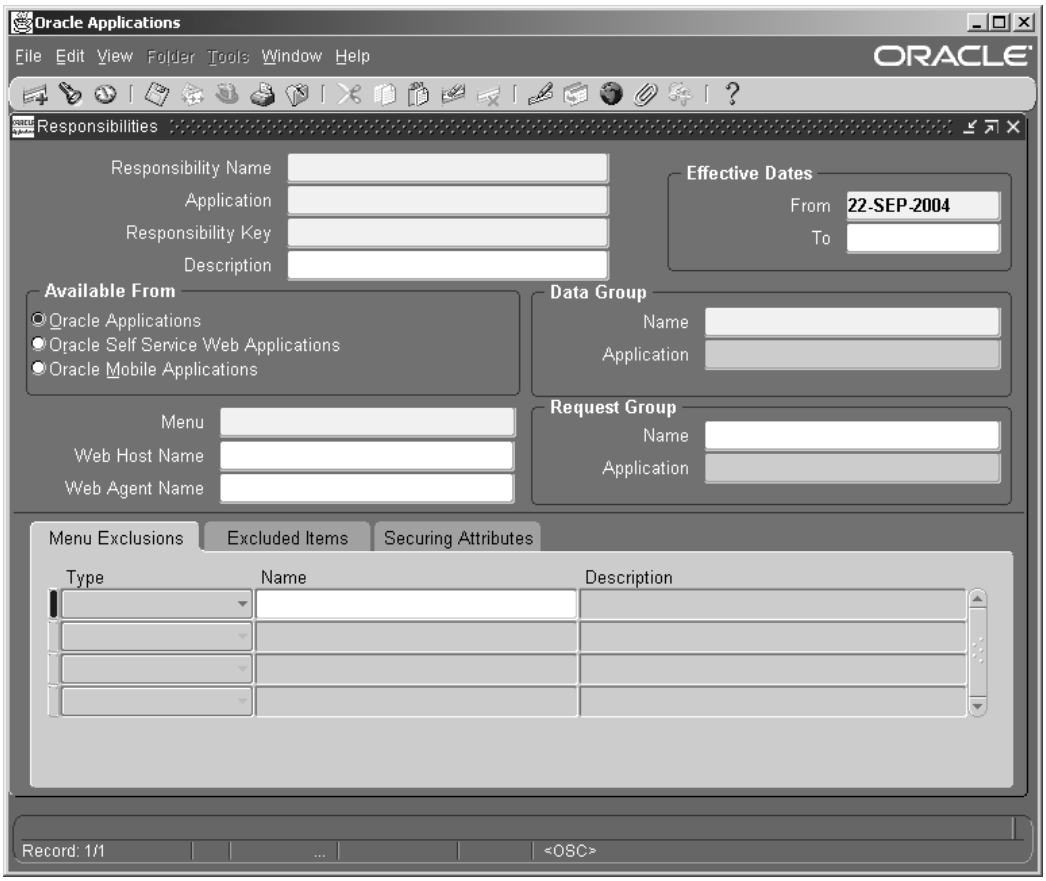
Implement data security by granting access to a set of functions (either a navigation menu or a permission set) to a user or group of users.

Data security policies can reflect access to:

- A specific instance (row) identified by a primary key value
- All instances (rows) of an object
- An instance set defined by a SQL predicate (WHERE clause)

Responsibilities Window

Responsibilities Window



Use this window to define a responsibility. Each application user is assigned at least one responsibility.

> **Note:** The information in this section can also be used to define a responsibility in the HTML-based Create Responsibility page.

A responsibility determines whether the user accesses Oracle E-Business Suite or Oracle Mobile Applications; which applications functions a user can use; which reports and concurrent programs the user can run; and which data those reports and concurrent programs can access.

Responsibilities cannot be deleted. To prevent a responsibility from being used, set the Effective Date's To field to a past date and restart Oracle E-Business Suite.

See: Overview of Function Security, page 4-11

Before defining your responsibility, do the following:

- Use the Data Groups window to list the ORACLE user name your responsibility's concurrent programs reference on an application-by-application basis.
- Use the Request Groups window to define the Request Group you wish to make available with this responsibility.
- Use the Menus window to view the predefined Menu you can assign to this responsibility.

Responsibilities Block

An application name and a responsibility name uniquely identify a responsibility.

Responsibility Name

If you have multiple responsibilities, a pop-up window includes this name after you sign on.

Application

The owning application for the responsibility.

This application name does not prevent the user of this responsibility from accessing other applications' forms and functions if you define the menu to access other applications.

Responsibility Key

This is the internal key for the responsibility that is used by loader programs, (concurrent programs that load messages, user profiles, user profile values, and other information into Oracle E-Business Suite tables). The responsibility key is unique per application.

Do not use non-ASCII characters in the responsibility key.

Also, avoid using the following characters in the responsibility key: !, ", ;, [,], (,), {, }, %, |, <, >.

Effective Dates (From/To)

Enter the start/end dates on which the responsibility becomes active/inactive. The default value for the start date is the current date. If you do not enter an end date, the responsibility is valid indefinitely.

You cannot delete a responsibility, because its information helps to provide an audit trail. You can deactivate a responsibility at any time by setting the end date to the current date. If you wish to reactivate the responsibility later, either change the end date to a date after the current date, or clear the end date.

Available From

This is the navigator from which the responsibility will be available (Oracle E-Business Suite forms navigator, mobile navigator).

A responsibility may be associated with only one Oracle E-Business Suite system.

Data Group

> **Note:** Data groups are used for backward compatibility only. Oracle Application Framework does not support the data groups feature. You should not define any custom data groups.

Name/Application

The data group defines the pairing of application and ORACLE user name.

Select the application whose ORACLE user name forms connect to when you choose this responsibility. The ORACLE user name determines the database tables and table privileges accessible by your responsibility. Transaction managers can only process requests from responsibilities assigned the same data group as the transaction manager.

Menu

The menu whose name you enter must already be defined with Oracle E-Business Suite. See: Menus, page 4-36.

Request Group - Name/Application

Specify a request security group to associate the responsibility to a set of requests, request sets, or concurrent programs that users logged in with this responsibility can run from the Submit Requests window. Note that such users can also access requests from a Submit Requests window you customize with a request group code through menu parameters

> **Note:** The Request Security Groups feature is provided for backward compatibility.
>
> New responsibilities should be created in accordance with Role-Based Access Control and should not have a default request security group.

See:

Overview of Oracle E-Business Suite Security, page 4-1

Customizing the Submit Requests Window Using Codes, *Oracle E-Business Suite Setup Guide*

Request Groups, *Oracle E-Business Suite Setup Guide*

Menu Exclusions Block

> **Note:** Menu exclusions should be used for backward compatibility only.

Define function and menu exclusion rules to restrict the application functionality accessible to a responsibility.

Type

Select either Function or Menu as the type of exclusion rule to apply against this responsibility.

- When you exclude a function from a responsibility, all occurrences of that function throughout the responsibility's menu structure are excluded.
- When you exclude a menu, all of its menu entries, that is, all the functions and menus of functions that it selects, are excluded.

Name

Select the name of the function or menu you wish to exclude from this responsibility. The function or menu you specify must already be defined in Oracle E-Business Suite.

HTML-Based Applications Security

Oracle HTML-based applications use columns, rows and values in database tables to define what information users can access. Table columns represent attributes that can be assigned to a responsibility as Securing Attributes or Excluded Attributes. These attributes are defined in the Web Application Dictionary.

Excluded Items

Use the List of Values to select valid attributes. You can assign any number of Excluded Attributes to a responsibility.

Securing Attributes

Use the List of Values to select valid attributes. You can assign any number of securing attributes to the responsibility.

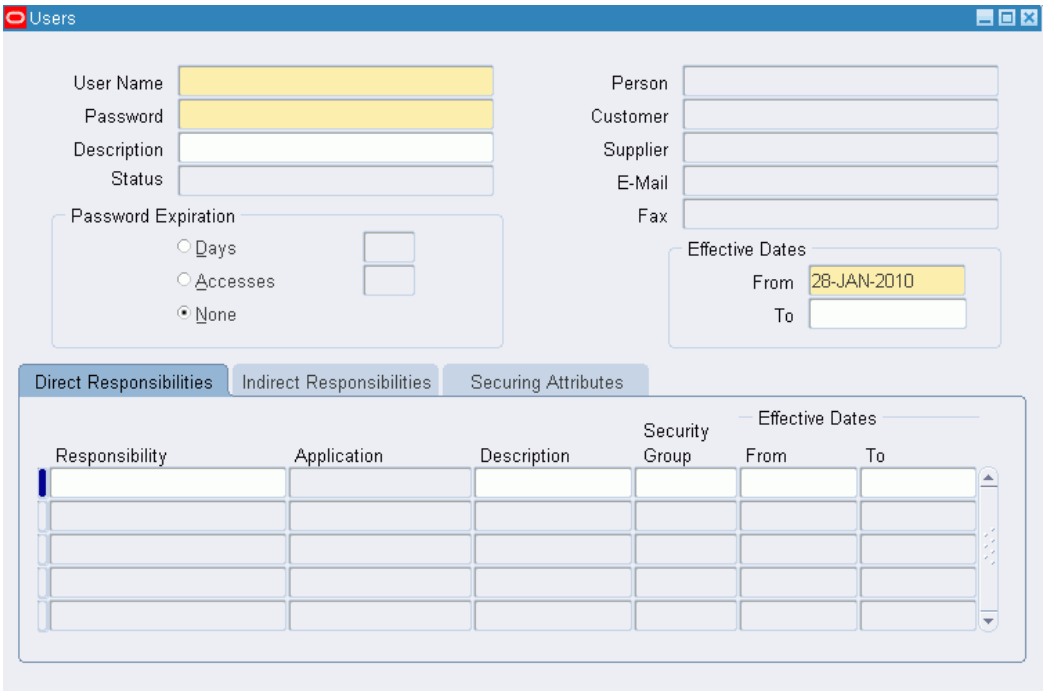
Security Groups Window

This form is for HRMS security only.

For more information on setting up system administration for the HRMS products, see: *Customizing, Reporting, and System Administration in Oracle HRMS.*

Users Window

Users Window



Use this window to define an Oracle E-Business Suite user. This user is an authorized user of Oracle E-Business Suite, and is uniquely identified by a user name.

Once defined, a new Oracle E-Business Suite user can sign on to Oracle E-Business Suite and access data through Oracle E-Business Suite windows.

> **Note:** If you have upgraded from a previous release of Oracle E-Business Suite, ensure that you have run the Party Merge concurrent program to update your user data. If you have no run this program, you may receive errors in querying your user data.
>
> For more information, see the Oracle Trading Community Architecture documentation.

Users Block

Enter these fields for the user.

User Name

An application user enters this user name to sign on to Oracle E-Business Suite.

The user name should only contain characters allowed by Oracle Single Sign-On.

> **Tip:** We recommend that you define meaningful user names, such as the employee's first initial followed by their last name. Or, for a group account, you can define the application user name so as to indicate the purpose or nature of the group account.

Password

Enter the initial password of an application user. An application user enters this password along with his user name to sign on to Oracle E-Business Suite.

- A password must be at least five (5) characters and can be up to thirty (30) characters.
- All characters are allowed except control characters, which are non-printable. Oracle encourages the use of non-alphanumeric characters because they add complexity, making passwords harder to guess.

This window does not display the password you enter. After you enter a password, you must re-enter it to ensure you did not make a typing error.

If the application user already exists and the two entries do not match, the original password is not changed and an error message is displayed.

If you are defining a new application user and the two entries do not match, you are required to enter the password again. For a new user, you cannot navigate to the next field until the two entries match.

The first time an application user signs on, he must change his password. If a user forgets his password, you can reassign a new password in this field.

As System Administrator, you can set an initial password or change an existing password, but you cannot access the user's chosen password.

You can set the minimum length of Oracle E-Business Suite user passwords using the profile option Signon Password Length. If this profile option is left unset, the minimum length defaults to 5.

You can set the minimum number of days that a user must wait before being allowed to reuse a password with the Signon Password No Reuse profile option.

You can use the profile option Signon Password Hard to Guess to set rules for choosing passwords to ensure that they will be "hard to guess." A password is considered hard-to-guess if it follows these rules:

- The password contains at least one letter and at least one number.

- The password does not contain the user name.
- The password does not contain repeating characters.

The Signon Password Failure Limit profile option determines the maximum number of login attempts before the user's account is disabled.

For information on case sensitivity in passwords, see: Case Sensitivity in Oracle E-Business Suite User Passwords, page 4-2.

Status

The Status field indicates the status of the user account. This field is display-only and values are generated by the system. This field is similar to Status in Oracle User Management for managing user accounts.

Possible statuses of a user account are:

- Unassigned - This status is used for the moment of creating a new user in the form, before committing the transaction. Since a user ID hasn't been assigned yet at that moment, the record status is Unassigned.
- Pending - This user account exists but cannot be used yet. For example, a user account with "Effective Dates" that are in the future would have a Pending status.
- Locked - This user account is locked. For example, if a user has unsuccessfully tried to log in over the maximum number of tries allowed (per the profile option "Signon Password FailureLimit"), then the user account becomes locked.
- Active - The status for a user account is Active if both of the following conditions are true:
  - The start date is not NULL and is before or equal to the current date
  - The end date is NULL or is after the current date
- Inactive - This user has an inactive account. For example, a user account with "Effective Dates" that are in the past would have an Inactive status.

Person, Customer, and Supplier

Use these fields to enter the name of an employee (person), customer, or supplier contact. Enter the last name and first name, separated by a comma, of the employee, customer, or supplier who is using this application user name and password. Use the List of Values to select a valid name.

For more information on using these fields, see the Oracle Trading Community Architecture documentation.

Email

Enter the email address for this user.

Fax

Enter the fax number for this user.

Password Expiration

- Days - Enter the maximum number of days between password changes. A pop-up window prompts an application user to change his password after the maximum number of days you specify has elapsed.

- Accesses - Enter the maximum allowed number of sign-ons to Oracle E-Business Suite allowed between password changes. A pop-up window prompts an application user to change their password after the maximum number of accesses you specify has elapsed.

  Tip: We recommend that you require all application users to make regular password changes. This reduces the likelihood of unauthorized access to Oracle E-Business Suite.

Effective Dates (From/To)

The user cannot sign on to Oracle E-Business Suite before the start date or after the end date. The default for the start date is the current date. If you do not enter an end date, the user name is valid indefinitely.

You cannot delete an application user from Oracle E-Business Suite because this information helps to provide an audit trail. You can deactivate an Oracle E-Business Suite user at any time by setting the End Date to the current date.

If you wish to reactivate a user, change the End Date to a date after the current date, or clear the End Date field.

Direct Responsibilities

Direct responsibilities are responsibilities assigned to the user directly.

Responsibility

Select the name of a responsibility you wish to assign to this application user. A responsibility is uniquely identified by application name and responsibility name.

Security Group

This field is for HRMS security only. See: *Customizing, Reporting, and System Administration in Oracle HRMS*.

This field is enabled only if the profile Enable Security Groups is enabled.

From/To

You cannot delete a responsibility because this information helps to provide an audit trail. You can deactivate a user's responsibility at any time by setting the End Date to the current date.

If you wish to reactivate the responsibility for the user, change the End Date to a date after the current date, or clear the End Date.

Indirect Responsibilities

Indirect responsibilities are used with Oracle User Management only. A user may "inherit" an indirect responsibility through membership of a group to which the responsibility has been assigned.

This block is read-only.

Securing Attributes

Securing attributes are used by some Oracle HTML-based applications to allow rows (records) of data to be visible to specified users or responsibilities based on the specific data (attribute values) contained in the row.

You may assign one or more values for any of the securing attributes assigned to the user. If a securing attribute is assigned to both a responsibility and to a user, but the user does not have a value for that securing attribute, no information is returned for that attribute.

For example, to allow a user in the ADMIN responsibility to see rows containing a CUSTOMER_ID value of 1000, assign the securing attribute of CUSTOMER_ID to the ADMIN responsibility. Then give the user a security attribute CUSTOMER_ID value of 1000.

When the user logs into the Admin responsibility, the only customer data they have access to has a CUSTOMER_ID value of 1000.

Attribute

Select an attribute you want used to determine which records this user can access. You can select from any of the attributes assigned to the user's responsibility.

Value

Enter the value for the attribute you want used to determine which records this user can access.

Related Topics

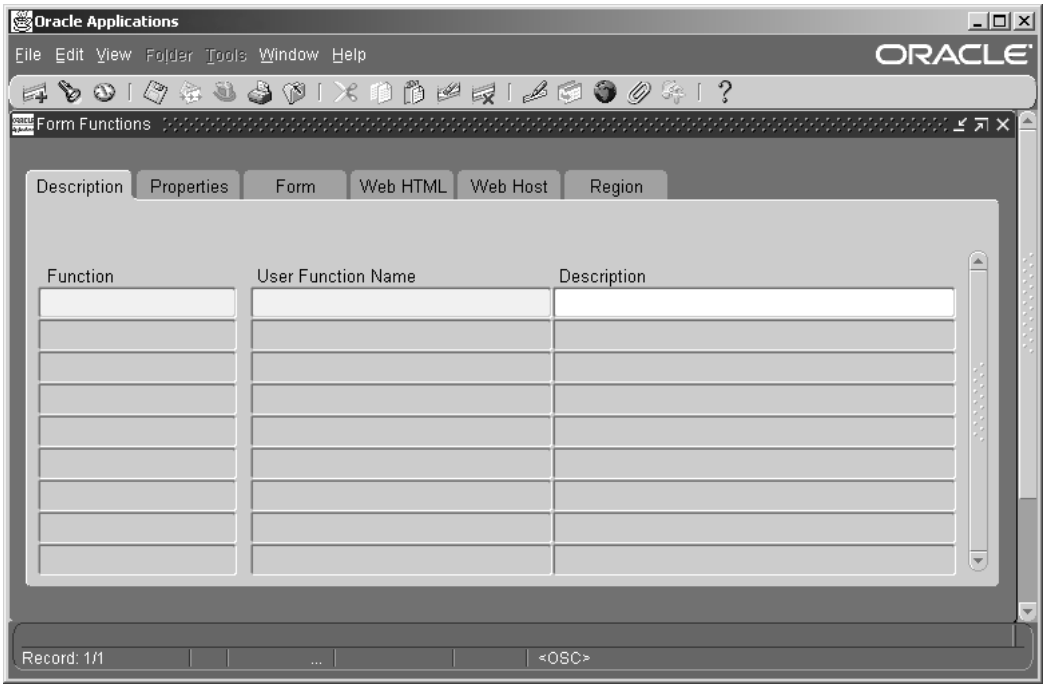
Defining a Responsibility, page 4-6

Overview of Function Security, page 4-11

Responsibilities, page 4-22

Form Functions Window

Form Functions Window



Used to define new functions. A function is a part of an application's functionality that is registered under a unique name for the purpose of assigning it to, or excluding it from, a responsibility.

Description

Fields include:

Function

Users do not see this unique function name. However, you may use this name when calling your function programmatically. You should follow the naming conventions for functions.

User Function Name

Enter a unique name that describes your function. You see this name when assigning functions to menus. This name appears in the Top Ten List of the Navigator window.

Properties

Fields include:

Type

A function's type describes its use. A function's type is passed back when a developer tests the availability of a function. The developer can write code that takes an action based on the function's type.

Standard function types include the following:

ADFX	External ADF Application. Used for linking an external Application Developer Framework (ADF) 11g application deployed on an Oracle Application Server 11g container from the Oracle E-Business Suite home page.
DBPORTLET	Database provider portlet.
FORM	Oracle E-Business Suite form functions are registered with a type of FORM.
JSP	Functions used for some products in the Oracle Self-Service Web Applications. These are typically JSP functions.
REST	REST service.
SERVLET	Servlet functions used for some products in the Oracle Self-Service Web Applications.
SUBFUNCTION	Subfunctions are added to menus (without prompts) to provide security functionality for forms or other functions.
WEBPORTLET	Web provider portlet.
WWK	Functions used for some products in the Oracle Self-Service Web Applications. These are typically PL/SQL functions

	that open a new window.
WWR or WWL	Functions used for some products in the Oracle Self-Service Web Applications.
WWJ	OA Framework JSP portlet.
WWW	Functions used for some products in the Oracle Self-Service Web Applications. These are typically PL/SQL functions.

For information on functions used by Oracle Application Framework, see My Oracle Support Knowledge Document 1315485.1, *Oracle Application Framework Developer's Guide*.

Maintenance Mode Support

This field should not be used. Maintenance Mode is disabled in an online patching-enabled environment.

Context Dependence

In general, the context dependence determines the required context for the function to work properly. The context dependence controls whether the user must choose a specified context (if not already in that context) before executing the function.

For example, some functions are controlled by profile options that affect what the user can perform within the current context. Types of context dependence are:

- **Responsibility** - The function is controlled by the user's responsibility (RESP_ID/RESP_APPL_ID (includes ORG_ID)).
- **Organization** - The function is controlled by the user's organization (ORG_ID).
- **Security Group** - The function is controlled by the user's security group (service bureau mode).
- **None** - There is no dependence on the user's session context.

Form

Fields include the following:

Form/Application

If you are defining a form function, select the name and application of your form.

Parameters

Enter the parameters you wish to pass to your function. Separate parameters with a

space.

For an executable (form) function:

- If you specify the parameter QUERY_ONLY=YES, the form opens in query-only mode. Oracle Application Object Library removes this parameter from the list of form parameters before opening the form in query-only mode.

- You can also specify a different form name to use when searching for help for a form in the appropriate help file. The syntax to use is:

  HELP_TARGET = "*alternative_form_name*"

  Your form name overrides the name of the form. See: Help Targets in Oracle E-Business Suite, *Oracle E-Business Suite Setup Guide*.

For a concurrent program submitted through the Standard Request Submission form, the following syntax may be used:

TITLE="*appl_short_name*:*message_name*"

where *appl_shortname*:*message_name* is the name of a Message Dictionary message. See: Customizing the Submit Requests Window using Codes, *Oracle E-Business Suite Setup Guide*.

> **Warning:** In general, system administrators should not modify parameters passed to predefined functions for Oracle E-Business Suite products. The few exceptions are documented in the relevant manuals or product notes.

Web HTML

The fields in the Web HTML and Web Host are only required if your function will be accessed from Oracle Application Framework. You do not need to enter any of these fields for functions based on Oracle Developer forms.

HTML Call

The last section of your function URL is the HTML Call. The HTML Call is used to activate your function. The function may be either a static web page or a procedure.

The syntax for this field depends on the function type.

For functions used with Mobile Application Server, enter the full name of your Java class file, including `<package name>.<class name>`. The class name and package name are case sensitive. Mobile Application Server will try to load this class from the classpath as it is. For example, 'oracle.apps.mwa.demo.hello.HelloWorld'.

Web Host

The fields in the Web HTML and Web Host are optional and only enabled for some types of functions. These fields apply only to Oracle Application Framework functions.

Host Name

The URL (universal resource locator) or address required for your function consists of three sections: the Host Name, Agent Name, and the HTML Call. The Host name is the IP address or alias of the machine where the Web server is running.

Agent Name

The second section of your function URL is the Oracle Web Agent. The Oracle Web Agent determines which database is used when running your function. Defaults to the last agent used.

Icon

Enter the name of the icon used for this function. If the function will be in the "Level 1" menu, provide the name of a seeded icon to assign to the function. The icon file must reside in the $OA_MEDIA directory. This icon displays when the profile FND: Top-Level Menu Display Mode is set to display the "Level 1" menu as icons and links, when the function appears in the global header, or when the function is a favorite on the simplified home page.

Secured

Secured is only required when your function is accessed by Oracle Workflow. Checking Secured enables recipients of a workflow email notification to respond using email.

Encrypt Parameters

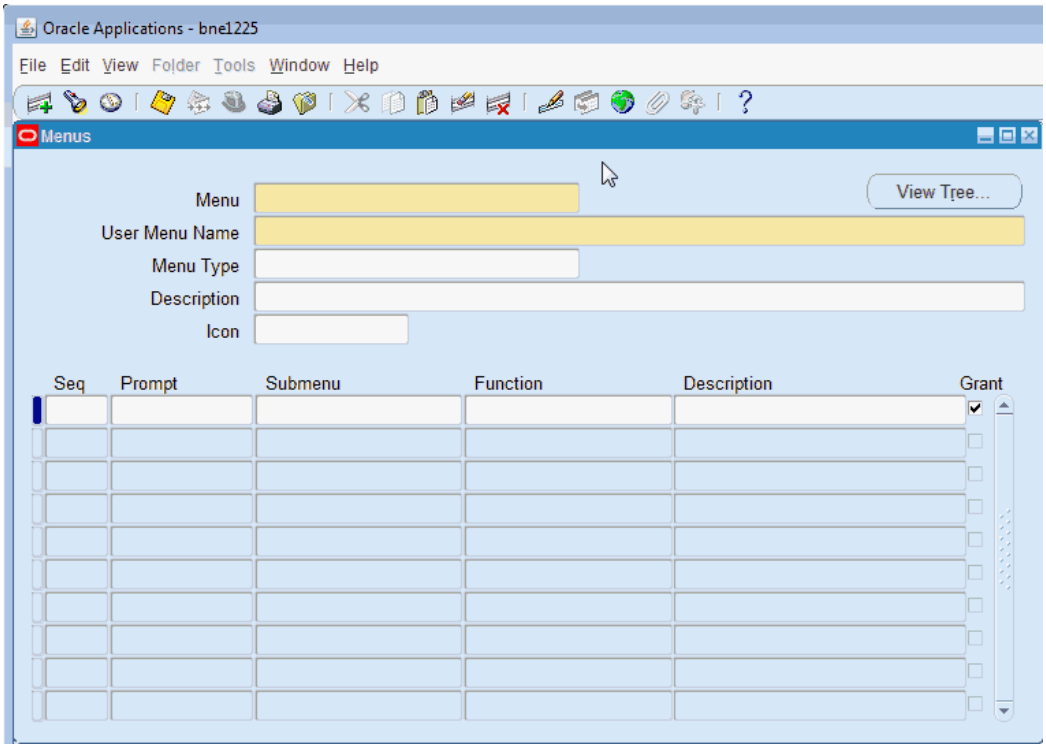
Checking Encrypt Parameters adds a layer of security to your function to ensure that a user cannot access your function by altering the URL in their browser window. You must define Encrypt Parameters when you define your function to take advantage of this feature.

Region

The fields on this page are for future use.

Menus Window

Menus Window



Used to define a new menu or modify an existing menu.

A menu is a hierarchical arrangement of functions and menus of functions. Each responsibility has a menu assigned to it.

You can build a custom menu for that responsibility using predefined forms. However, we recommend that you do not disassociate a form from its developer-defined menus.

After you save your changes in this form, a request is submitted to compile the menu data.

See:

Overview of Function Security, page 4-11

Implementing Function Security, page 4-16

Before you define your menu, perform the following:

- Register your application using adsplice. See: AD Splicer, *Oracle E-Business Suite Setup Guide* and My Oracle Support Knowledge Document 1577707.1, *Creating a Custom Application in Oracle E-Business Suite Release 12.2*.

- Register any forms you wish to access from your menu with Oracle Application Object Library using the Forms window.
- Define any functions you intend to call from your menu.
- Define any menus that you intend to call from your menu. Define the lowest-level submenus first. A submenu must be defined before it can be called by another menu.

  Tip: By calling submenus from your menu, you can group related windows together under a single heading on your menu. You can reuse your menu on other menus.

Menus Block

Menu entries detail the options available from your menu.

Menu

Choose a name that describes the purpose of the menu. Users do not see this menu name.

Note: Once the menu is saved, this menu name cannot be updated.

View Tree...

Once you have defined a menu, you can see its hierarchical structure using the "View Tree..." button. See: Menu Viewer, page 4-39.

User Menu Name

You use the user menu name when a responsibility calls a menu or when one menu calls another.

Menu Type

Specify a menu type to describe the purpose of your menu. Options include:

- Standard - for menus that would be used in the Navigator form
- Tab - for menus used in self service applications tabs
- Security - for menus that are used to aggregate functions for data security or specific function security purposes, but would not be used in the Navigator form

In addition, see the section on Oracle Application Framework menu types, page 4-55.

Icon

If this menu will be an item on a "Level 1" menu, provide the name of a seeded icon to assign to the menu. This icon displays when the profile FND: Top-Level Menu Display Mode is set to display the "Level 1" menu as icons and links.

Menu Entries Block

Fields include the following:

Sequence

Enter a sequence number to specify where a menu entry appears relative to other menu entries in a menu. The default value for this field is the next whole sequence number.

> **Important:** You can only use integers as sequence numbers.

A menu entry with a lower sequence number appears before a menu entry with a higher sequence number.

You cannot replace a menu entry sequence number with another sequence number that already exists. If you want to add menu entries to a menu entry sequence, carefully renumber your menu entries to a sequence range well outside the sequence range you want, ensuring that you do not use existing sequence numbers. If you want to renumber an entry, then delete the entire row and save your work; and then insert a new row with the desired sequence number and same prompt and submenu/function as the previous one.

Navigator Prompt

Enter a user-friendly, intuitive prompt your menu displays for this menu entry. You see this menu prompt in the hierarchy list of the Navigator window.

> **Tip:** Enter menu prompts that have unique first letters so that power users can type the first letter of the menu prompt to choose a menu entry.

Submenu

Call another menu and allow your user to select menu entries from that menu.

Function

Call a function you wish to include in the menu. A form function (form) appears in the Navigate window and allows access to that form. Other non-form functions (subfunctions) allow access to a particular subset of form functionality from this menu.

Description

Descriptions appear in a field at the top of the Navigate window when a menu entry is highlighted.

Grant

The Grant checkbox should usually be checked. Checking this box indicates that this menu entry is automatically enabled for the user. If this is not checked then the menu entry must be enabled using additional data security rules.

For more information on grants, see: Overview of Data Security, page 4-18 and Grants, page 4-47.

Menu Viewer

The Menu Viewer is a read-only window that provides a hierarchical view of the submenus and functions of a menu, and also lists properties of the menus and functions.

You can launch the viewer from the Menus form by clicking on the "View Tree..." button. The viewer will appear for the menu specified in the Menus form.

> **Note:** When you are creating or editing a new menu, your changes must be committed to the database before you will be able to see them in the Menu Viewer.

Functionality

The Menu Viewer consists of two panes, one showing the menu tree and the other the node properties.

Menu Tree

To view the menu tree, click on the plus (+) sign next to the menu. You will see a hierarchical tree with a number of nodes. Each node represents a function or submenu of your main menu.

> **Note:** The menu tree displays the user menu name for the main menu, and displays the prompts from the Menus form for submenus and functions. If no prompt has been specified, then no label will appear for the node.

To print a menu tree, choose **Print** from the File menu.

Node Properties

To view properties of a particular menu or function, highlight the node in the menu tree. The node properties will appear in the Properties pane. You can create a separate Properties page for a node by clicking the "push pin" button at the top of the Properties pane.

The entry's sequence number, prompt, and description are shown.

View Options

The View menu provides options on how the viewer displays your menu.

You can specify whether the Node Properties pane, the toolbar, or the status bar are displayed. You can also choose the display style in which you view your menu tree.

Display Styles

There are three styles for viewing your menu tree. You can select one from the View menu or from the buttons on the toolbar.

Vertical	Menu entries are displayed vertically, similar to how they appear in the Navigator window when you log on to Oracle E-Business Suite.
Interleaved	Menu entries are displayed horizontally and vertically.
Org-Chart	Menu entries are displayed horizontally as in an organizational chart.

Edit Menu

From the Edit menu you can bring up a Properties window for the node you have highlighted in the menu tree.

> **Note:** You can view the properties for your menu or function here, but you cannot edit them.

You can view and edit your Preferences for the Menu Viewer. You can choose colors for your menu tree pane as well as the text font and size.

Objects

Use these pages to find, create, and edit data objects. You define objects to be secured in the Data Security system.

Objects can be tables or views. An object must be queryable in SQL, and the combination of primary key columns specified must be a unique key.

In these pages, objects are described with the following

- The **Name** is the name that appears in the Object Instance Set and Grants pages. This name should be user-friendly.
- The **Code** is the internal name of the object.
- The **Application Name** is the owning application.
- The **Database Object Name** is the name of the underlying database object.

Related Topics

Overview of Data Security, page 4-18

Find Objects

Use this page to find an existing object.

Simple Search

Name

The display name of the object.

Code

The object name.

Application Name

The object's owning application.

Database Object Name

The database object name.

Advanced Search

Use the Advanced Search screen to find data that meet a set of criteria. With the Advanced Search screen, you can enter in special conditions based on the given fields, and the search results will consist of all data that match the conditions.

For example, for a specified application, you can search for all objects whose name begins with a letter before "P." (Note: all uppercase letters precede all lowercase letters for this type of search).

Search Results

The search results are shown in a table with the following columns:

- Name - click on the object name to view details on the object.
- Code
- Application Name
- Database Object
- Description
- Last Update

To update an object, click on the icon under the Update column.

Update Object

Use this page to update the fields listed below for an object. You cannot change the internal Object Name of an existing object.

Display Name

Enter a user-friendly name for the object.

Application Name

The owning application for the object. This application owns the database table on which the object is based.

Database Object Name

Typically this is a table in the database.

Description

Enter a description for the object.

Create Object

Use this page to create a new object. Enter the following information:

Name

Enter a user-friendly name for the object.

Code

Enter a code that will be used as an internal name for the object. This name cannot include spaces and can include underscores and hyphens. You cannot update the object name after the object is created and saved.

Application Name

The owning application for the object. This application owns the database table on which the object is based.

Database Object

Typically this is a table in the database.

Description

Enter a description for the object.

Object Column Details

Enter in information on the primary key for the object (*n* below indicates an integer between 1 and 5). The primary key is used to identify rows (object instances) for inclusion in object instance sets.

PK*n* Column Name

The primary key column name.

PK*n* Column Type

The datatype for the column.

Object Detail

This page provides the following information for an object:

- Object Name
- Display Name
- Application
- Database Object Name
- Description

Columns

You can also view details on columns that comprise the primary key (*n* below indicates an integer between 1 and 5):

- PK*n* Column Name
- PK*n* Column Type

Instances of an object can be grouped together into an object instance set. For example, you may want to create a group of projects or a group of items. To create and manage objects instance sets, click **Manage Object Instance Sets**.

Click on the "Return to Object Search" link to go back to the main Objects page.

Delete Object

Confirm the deletion of an object from this page. Review the information shown, and click **Delete**.

Related Topics

Object Details, page 4-43

Object Instance Sets

After you create an object you can create a set of instances of the object. For example, you could define the object "User" corresponding to the User table. Each row in the User table becomes an instance of the User object. Users in the sales organization could then be grouped into an Object Instance Set named "Sales Organization."

Object Instance Sets are described by the following:

- The **Object Instance Set Name** is its internal name. This name must not contain any spaces and can include underscores.
- The **Display Name** is a user-friendly name for the object that appears in the Grants pages.
- The **Predicate** is the WHERE clause used to define the object instances in the set. It must be a valid SQL predicate for the database object.

Manage Object Instance Set

Use this page to manage existing object instance sets or create new ones.

The following object information is displayed:

- Object Name
- Display Name
- Application
- Database Object Name
- Description

Existing Object Instance Sets

- Instance Set Name - click on the Instance Set Name to view details
- Display Name
- Description

To update an object, click on the icon under the Details column to open up the Update Object page.

To delete a row, click on the icon under the Delete icon, or select the object and click **Delete**.

To return to the main Objects page, click on the "Return to Object Search" link.

Related Topics

Objects, page 4-40

Create Object Instance Set

The containing object's Name, Display Name, Application ID, Database Object Name, and Description are shown.

Enter the following for the Object Instance Set:

Code

Enter a name that will be used internally for the object instance set. This name cannot include spaces and can include underscores and hyphens. The Object Instance Set Name cannot be updated once the object instance set has been created and saved.

Name

Enter a user-friendly, descriptive name to appear in the Grants pages.

Description

Enter a description for the object instance set.

Predicate

This predicate determines which object instances are included in the set. Do not include "WHERE" in your entry, but only the body of the WHERE clause.

Update Object Instance Set

The containing object's Name, Display Name, Application ID, Database Object Name, and Description are shown.

> **Note:** The Object Instance Set Name cannot be updated after the object instance set has been created and saved.

Display Name

Enter a user-friendly, descriptive name to appear in the Grants pages.

Description

Enter a description for the object instance set.

Predicate

This predicate determines which object instances are included in the set. Do not include "WHERE" in your entry, but only the body of the WHERE clause.

Delete Object Instance Set

Confirm the deletion of an object from this page. Review the information shown, and click **Delete**.

Related Topics

Object Instance Set Details, page 4-46

Object Instance Set Details

Details of an object instance set are shown on this page.

The containing object's Name, Display Name, Application ID, Database Object Name, and Description are shown.

The following is shown for the object instance set:

- Code
- Name

- Description
- Predicate

Use the "Return to Manage Object Instance Sets" to return to the main page.

Related Topics

Object Instance Sets, page 4-44

Grants

The HTML-based pages for maintaining Grants can be accessed from the Functional Administrator responsibility. For more information on this responsibility, see:Overview of Functional Administrator and Functional Developer Responsibilities, *Oracle E-Business Suite Maintenance Guide*.

Search Grants

Use this page to search for grants.

You can search using the following criteria:

- Name
- Grantee Type - Select from one of the following:
  - All Users - The grant applies to all users.
  - Group of Users - The grant applies to a group of users.
  - Specific User - The grant applies to a single user.

    If you select Group of Users or Specific User, you will be prompted to specify the group or the user.
- Set - The Navigation Menu or Permission Set included in the grant.
- Object Type - A grant can apply to either all objects or only a specific object. Under Object Type, specify if your search should include only grants that apply to all objects ("All Objects"), only grants that apply to a specific object ("Specific Object"), or both ("Any").

  If you select Specific Object, you will be prompted to specify the object.
- Effective Dates.

Create Grant

Use these pages to create a grant. Grants are used to manage user access to product functionality. In these pages you give access to functions to specified users.

Related Topics

Overview of Data Security, page 4-18

Define Grant

In this page you specify basic information for the grant.

To define a grant:

1. Enter a name and description for your grant.
2. Enter effective dates for your grant.
3. Enter the security context information.

   The security context defines the circumstances in which the grant is active.

   For Grantee, you can select a single user, a role, or global (all users and roles).
4. For Operating Unit, specify an operating unit if you want your grant to apply to a specific one.
5. For Responsibility, specify a responsibility if you want your grant to apply to a specific one.
6. Enter the Data Security information if you are creating a data security policy for an object. The grant applies to the object you specify.

   If you are not creating a data security policy, you will skip the next step.

   > **Note:** You cannot change a data security policy once it has been saved. You can delete it or provide an end date to a data security policy.

Select Object Data Context

If you specified that your grant applies to a single object, you add context for that object in this page.

Choose one of the following:

- Global (All Rows) - Indicates that the set of functions is being granted for all rows of the object (for a function security grant).

- Instance - Indicates that the set of functions are being granted for a single row, specified by value(s) for the primary key.
- Instance Set - Indicates that the set of functions are being granted for a set of rows which is specified by an instance set predicate.

Define Object Parameters and Select Set

If you selected either an object instance or an instance set earlier, you can further customize the resulting set by additional information for the data context.

Additionally, you can select either a permission set or a navigation menu that can additionally specify how the grant will be applied in the security context.

For an instance set:

1. In the Predicate region, the predicate that defines the instance set is shown. In the Instance Set Details region, specify the values for the parameters to be used in the predicate above.
2. Select the permission set or navigation menu set that defines the grantee's access.

For an instance:

1. In the Instance Details region, specify information identifying the instance.
2. Select the permission set or navigation menu set that defines the grantee's access.

Review and Finish

Use this page to review the definition of your grant. Click **Finish** to save your work.

Update Grant

Use this page to update the definition of your grant.

Define a Grant

The following procedure summarizes the steps for defining a grant.

1. Log in to the Functional Administrator responsibility. The Grants page appears.
2. Click **Create Grant**.
3. In the Grant: Define Grant page, enter a grant name, description, and effective dates.
4. Select the grantee type, either **All Users**, **Group of Users** with a role or responsibility as the grantee, or **Specific User** with a user as the grantee. You can

also specify a responsibility or operating unit context. For example:

- If you use a custom responsibility, then select **Group of Users** in the Grantee Type field and select the applicable responsibility in the Grantee field.
- If you provide access through a user account, then select **Specific User** in the Grantee Type field and the name of the user in the Grantee field.
- If you provide access through an operating unit, then select **All Users** in the Grantee Type field and select the operating unit.

5. If the grant applies for a specific object, select the object in the Data Security region.
6. Click **Next**. If you specified an object for a data security policy, then the Grant: Select Object Data Context page appears. If you did not specify an object, skip to step 11.
7. Specify the rows of the object for which the set of functions is being granted by selecting **Global (All Rows)**, **Instance** (a single row), or **Instance Set** (a set of rows). If you selected **Instance Set**, specify the instance set you want to use.
8. Click **Next**. The Define Object Parameters and Select Set page appears.
9. For an instance, specify the primary key value that identifies the row.
10. For an instance set, enter the parameters for the predicate that defines the rows in the instance set.
11. For all grants, in the Set region, select the permission set or menu navigation set that defines the grantee's access.
12. Click **Next**.
13. In the Grant: Review and Finish page, review the grant details and click **Finish**.

View Grant

Use this page to view details for a grant, including:

- Security Context
- Object information, if applicable
- Set information

You can update or delete a grant from this page.

Functions

Use these pages to define new functions. A function is a part of an application's functionality that is registered under a unique name for the purpose of assigning it to, or excluding it from, a responsibility.

You can search for functions from the main page.

Function Types

When you define a function, you assign it one of the following types:

- External ADF Application - Used for linking an external Application Developer Framework (ADF) 11g application deployed on an Oracle Application Server 11g container from the Oracle E-Business Suite home page.
- Database Provider Portlet
- Form - an Oracle Forms form function.
- JSP Interoperable with OA
- SSWA JSP function
- Mobile Application - A function used in an Oracle mobile application.
- Process
- REST service - Used for REST services. For more information on REST services and other Oracle Application Framework functions, see the *Oracle Application Framework Developer's Guide*, available from My Oracle Support Knowledge Document 1315485.1.
- SSWA servlet function
- Web Provider portlet
- SSWA PL/SQL function that opens a new window (kiosk mode)
- Plug
- Generic Plug
- SSWA PL/SQL function

Related Topics

Form Functions Window, page 4-31

Search

Using Simple Search, You can search for functions using the following criteria:

- Name
- Code
- Type

Advanced Search

Using Advanced Search, you can be more flexible with your criteria, as well as search on the description field.

Create Function

Use these pages to create a function.

1. Specify a name for the function.
2. Specify a code for the function. The code is the internal name for the function. Once the function has been saved, the code cannot be updated.
3. Specify a type for the function.
4. For context dependence, specify 'None' or Responsibility.
5. If you are defining a form function, select the name and application of your form. If the function applies to a specific object, select the object name and specify parameters.
6. If you are using type "JSP Interoperable with OA," enter the values for the following properties in the **Create Function: Details** page.
   - HTML Call - provides the mapping to the associated page. At runtime, whenever this function is invoked, the OA Framework knows to display the page identified in this property.
   - Icon - if the function will be in the "Level 1" menu, provide the name of a seeded icon to assign to the function. The icon file must reside in the $OA_MEDIA directory. This icon displays when the profile FND: Top-Level Menu Display Mode is set to display the "Level 1" menu as icons and links.

If the function applies to a specific object, select the object name and specify parameters. For more details, see: *Oracle Applications Framework Developer's Guide*.

> **Note:** The Maintenance Mode Support field is not used. Maintenance Mode is disabled in an online patching-enabled environment.

Update Function

Use this page to update an existing function. Note that you cannot update the code for an existing function.

To update a function:

1. Specify a name for the function.
2. If this function applies to a specific object, specify the object.
3. Specify a type for the function.
4. For context dependence, specify 'None' or Responsibility.

> **Note:** The Maintenance Mode Support field is not used. Maintenance Mode is disabled in an online patching-enabled environment.

To update function details:

1. If this is a form function, select the name and application of your form.
2. If the function applies to a specific object, you can update the object name and specify parameters.

In updating menus,

- You can remove the function from menus containing it using the Menus subtab.
- You can also update menu prompts and descriptions for the function here.

Duplicate Function

Use this page to duplicate an existing function.

Note that you must enter a unique code for the new function you are creating.

To duplicate a function:

1. Specify a name for the function.
2. Specify a code for the function. The code is the internal name for the function. Once

the function has been saved, the code cannot be updated.

3. Specify a type for the function.

4. For context dependence, specify 'None' or Responsibility.

5. If you are defining a form function, select the name and application of your form. If the function applies to a specific object, select the object name and specify parameters.

   Note: The Maintenance Mode Support field is not used. Maintenance Mode is disabled in an online patching-enabled environment.

View Function

Use this page to view details on an existing function.

You can update and duplicate a function from this page. If the function is not on a menu, you can also delete the function.

Delete Function

Use this page to delete a function.

Navigation Menus

Define a new menu or modify an existing menu.

A menu is a hierarchical arrangement of functions and menus of functions. Each responsibility has a menu assigned to it.

You can build a custom menu for that responsibility using predefined forms. However, we recommend that you do not disassociate a form from its developer-defined menus.

Before creating a menu, perform the following:

- Register your application using adsplice. See: AD Splicer, *Oracle E-Business Suite Setup Guide* and My Oracle Support Knowledge Document 1577707.1, *Creating a Custom Application in Oracle E-Business Suite Release 12.2*.

- Define any menus that you intend to call from your menu. Define the lowest-level submenus first. A submenu must be defined before it can be called by another menu.

  Tip: By calling submenus from your menu, you can group related windows together under a single heading on your menu. You can

reuse your menu on other menus.

Terms

Terms used in defining menus include:

- Name - The display name for the menu
- Code - The internal name for the menu
- Type - The purpose of the menu
  - Permission Set - For menus that are used to aggregate functions for data security or specific function security purposes, but would not be used in the Navigator form.
  - Standard - For menus used in the Navigator form
  - App Pref Menu Container - For preferences
  - Global Menu - For providing access to tasks and content that are applicable to the entire application
  - HTML Side Navigator Menu
  - HTML SideBar
  - HTML SideList
  - HTML Sub Tab - A tab-like control for switching content or action views in the page's content area. Sub tabs can be used with a horizontal navigation element, with a tab and horizontal navigation elements, or with a side navigation
  - HTML Tab
  - Homepage

If you are creating a menu to be used with Oracle Application Framework, see My Oracle Support Knowledge Document 1315485.1, *Oracle Application Framework Developer's Guide*.

Search for Menus

Enter any of the following criteria for the menu:

- Name

- Code
- Type

Create Navigation Menu

Use this page to create a navigation menu.

1. Choose a user-friendly name that describes the purpose of the menu.
2. Enter a code for the menu. Choose an internal name that indicates the purpose of the menu. Users do not see this menu code.
3. Optionally specify a menu type and description to describe the purpose of your menu.
4. If this menu will be an item on a "Level 1" menu, provide the name of a seeded icon to assign to the menu. This icon displays when the profile FND: Top-Level Menu Display Mode is set to display the "Level 1" menu as icons and links.

Add your information for your menu entries using the Menu Builder.

1. Enter a prompt for your menu entry.

   Enter a user-friendly, intuitive prompt your menu displays for this menu entry. You see this menu prompt in the hierarchy list of the Forms Navigator window.

   > **Tip:** Enter menu prompts that have unique first letters so that power users can type the first letter of the menu prompt to choose a menu entry.

2. If this menu entry is a menu itself (a submenu), enter in the menu name.

   You can call another menu and allow your user to select menu entries from that menu.

3. If this menu entry is a function, enter in the function name.

   Call a function you wish to include in the menu.

4. Specify the function type.
5. Apply your changes.

If you want to reorder the menu entries, click **Reorder** .

Menu Manager

Once you have your menu defined, you can update its list of entries in the Menu

Manager tab.

Hierarchy of Children

The Hierarchy of Children subtab provides information on the child nodes within the menu structure. Child nodes are either functions or menus (submenus). Child nodes are displayed in a hierarchy with the following information, as applicable: display name, internal menu name, function name, type, and description.

Direct Parents

The Direct Parents subtab allows the user to see the direct parent(s), if any, of the navigation menu. A direct parent is a menu that contains this menu directly as a submenu. This feature is useful in identifying the direct impact of any changes that may be made to this menu.

For each parent, the prompt and internal menu name is shown.

Grants

The Grants subtab displays the associated grants that secure the navigation menu.

For each associated grant the following is shown: name, grantee type, grantee, valid dates, data context type, object, and instance set.

Update Menu

Use this page to update an existing navigation menu.

All fields can be updated except for the menu code.

The direct parents of a menu can be deleted in the Direct Parents tab.

You cannot update a parent menu from this tab. You must navigate to the parent menu record itself to update it.

> **Note:** You cannot replace an existing parent menu with another menu, as the parent menu is used as the primary key of the hierarchy mapping. Instead, you have to delete this existing (child) menu and add a new menu. Also, the sequence number cannot be updated since it is the primary key. You can update the prompt and description.

Duplicate Menu

Use this page to duplicate a menu and copy its hierarchy of children. You must give the duplicate menu and new code (internal name).

View Menu

Use this page to view details of a menu.

Delete Menu

Use this page to delete a menu.

Note that you cannot delete a referenced menu. A menu can be referenced by any of the following:

- Children (menu or function)
- Menu parents
- Grants

Permissions

A permission is the smallest unit of securable action that can be performed on the system. A permission can either be abstract permissions or executable functions (menu). It can either be a system level permission or be sensitive to a data context. For example, a particular JSP page may be an executable permission and "View Person" may be an abstract permission.

The Permissions pages can be accessed from the Functional Administrator and Functional Developer responsibilities. For more information on these, see:Overview of Functional Administrator and Functional Developer Responsibilities, *Oracle E-Business Suite Setup Guide*.

You can search for permissions from the main page. You can update, duplicate, or remove a permission found in your search results. You can also create a new permission from this page.

Search for permissions using the following criteria:

- Name
- Code
- Object Name

Create Permission

Use these pages to create a permission.

1. Specify a name for the permission.

2. Specify a code for the permission. The code is the internal name for the permission. Once the permission has been saved, the code cannot be updated.

3. If this permission applies to a specific object, specify the object.

4. If you want to add this permission to a permission set now, select a permission set.

Update Permission

Use this page to update an existing permission.

Note that you cannot update the code (internal name) for the permission.

1. You can specify a new name for the permission.

2. You can specify a new object if the permission applies to a specific object.

You can update the permission set information as well:

1. To add this permission to a permission set, select a permission set from the list of values for "Add this to a Permission Set."

2. To delete this permission from a permission set, select the permission set in the table and click **Remove**.

Select **Apply** to save your changes.

Duplicate Permission

Use this page to duplicate an existing permission.

Note that you must enter a unique code for the new permission you are creating.

1. Specify a name for the permission.

2. Specify a code for the permission. The code is the internal name for the permission. Once the permission has been saved, the code cannot be updated.

3. If this permission applies to a specific object, specify the object.

4. If you want to add this permission to a permission set now, select a permission set.

View Permission

Use this page to view details on an existing permission.

You can update or duplicate a permission from this page. You can delete a permission from this page if it does not belong to a permission set.

Delete Permission

Use this page to delete a permission.

Permission Sets

Permission sets provide a way to group related permissions together. You can create a new permission set from this page.

The Permission Sets HTML-based pages can be accessed from the Functional Administrator and Functional Developer responsibilities. For more information on these, see:Overview of Functional Administrator and Functional Developer Responsibilities, *Oracle E-Business Suite Setup Guide*.

You can search for permission sets using the following criteria:

- Name
- Code

You can update, duplicate, or delete permission sets found in your search.

Create Permission Set

Use this page to create a permission set.

1. Specify a name for the permission set.
2. Specify a code for the permission set. The code is the internal name for the permission set. Once the permission set has been saved, the code cannot be updated.

Use the **Permission Set Builder** to add permissions to your new permission set. You can also add existing permission sets to the new permission set.

Update Permission Set

Use this page to update an existing permission set.

You can specify a new name for the permission set. Note that you cannot update the code (internal name) for the permission set.

If you want to update which permissions and permission sets belong to this permission set, use the **Permission Set Builder** to do so.

Permission Set Manager

Once you have your permission set defined, you can update the contents of the permission set in the Permission Set Manager tab.

Hierarchy of Children

The Hierarchy of Children subtab provides information on the child nodes in the permission set structure. A child node is either a permission or permission set. Child nodes are displayed in a hierarchy with the following information: display name, permission set name (if applicable), permission name (if applicable), and description.

Direct Parents

The Direct Parents subtab allows you to see the permission sets, if any, that include the current permission set. This feature is useful in identifying the direct impact of any changes that may be made to this permission set.

Grants

The Grants subtab displays the associated grants that secure the navigation menu.

For each associated grant, the name, grantee type, grantee, valid dates, data context type, object name, and instance set name is displayed.

Duplicate Permission Set

Use this page to duplicate an existing permission set.

Note that you must enter a unique code for the new permission set you are creating.

1. Specify a name for the permission set.
2. Specify a code for the permission set. The code is the internal name for the permission set. Once the permission set has been saved, the code cannot be updated.

If you want to update which permissions and permission sets belong to this permission set, use the **Permission Set Builder** to do so.

View Permission Set

Use this page to view details on an existing permission set.

Click **Update** to update the permission set.

Delete Permission Set

Use this page to delete a permission set. If a permission set is a child of another permission set, it cannot be deleted without first being removed from its parent permission set.

Compile Security Concurrent Program

Use this concurrent program to compile your menu data. Compiling your menu data allows for the system to determine more quickly whether a function is available to a particular responsibility/menu.

A request to run this program is automatically submitted when you make changes using the Menus form.

Parameter

Everything

This parameter takes the value Yes or No. "No" is used to recompile only those entities that are marked as needing recompilation. "Yes" is used to recompile all entities, and can take a long time. "No" is the default value.

Function Security Reports

Use the function security reports to document the structure of your menus. You can use these reports as hardcopy to document your customized menu structures before upgrading your Oracle E-Business Suite software.

The function security reports consist of the Function Security Functions Report, the Function Security Menu Report, and the Function Security Navigator Report.

These reports are available through the Function Security Menu Reports request set. For each report, specify the responsibility whose function security you want to review.

> **Note:** If a function and a menu are associated with the same menu entry and the function is excluded then the submenu and its children are also excluded.
>
> If the submenu is also included on another branch of the menu (same level or higher) than the submenu and functions will be included and should be on the reports assuming all other function security conditions are met.

Function Security Function Report

Specify a responsibility when submitting the report. The report output lists the functions accessible by the specified responsibility.

The report does not include items excluded by function security rules.

Function Security Menu Report

Specify a responsibility when submitting the report. The report output lists the complete menu of the responsibility, including all submenus and functions.

The report indicates any excluded menu items with the rule that excluded it.

Function Security Navigator Report

Specify a responsibility when submitting the report. The report output lists the menu as it appears in the navigator for the responsibility specified.

This report does not include items excluded by function security rules, or non-form functions that do not appear in the navigator.

Users of a Responsibility Report

This report documents who is using a given responsibility. Use this report when defining or editing application users.

Report Parameters

Application Name

Choose the name of the application to which the responsibility you want in your report belongs.

Responsibility Name

Choose the name of the responsibility you want in your report.

Report Heading

The report heading indicates the application name and responsibility for which you requested a report.

Column Headings

User Name

The name of the user who is assigned to the responsibility.

Start Date

The date the responsibility became active for the user.

End Date

The date the responsibility either becomes inactive or became inactive for the user. If no end date appears for a user, then this responsibility is always enabled for the user.

Description

The description of the user who is assigned to the responsibility.

Related Topics

Overview of Oracle E-Business Suite Security, page 4-1

Defining a Responsibility, page 4-6

Overview of Function Security, page 4-11

Responsibilities field help, page 4-22

Users field help, page 4-26

Active Responsibilities Report

This report shows all the responsibilities that are currently active, the users who can currently access each responsibility, and the start and end dates when they can access the responsibility.

Report Parameters

None.

Report Heading

This displays the name of the report, the date and time the report was run, and the page number.

Column Headings

Application Name

The name of the application associated with the responsibility.

Responsibility Name

The name of the currently active responsibility.

User Name

The name of the user who can currently access the responsibility.

Start Date

The date when the user can begin accessing the responsibility.

End Date

The date when the user can no longer access the responsibility. See: Overview of Oracle E-Business Suite Security, page 4-1.

Related Topics

Overview of Oracle E-Business Suite Security, page 4-1

Defining a Responsibility, page 4-6

Responsibilities field help, page 4-22

Users field help, page 4-26

Active Users Report

This report shows all the user names that are both currently active and have at least one active responsibility. It also displays all the responsibilities that users can access, and the start and end dates when they can access each responsibility.

Report Parameters

None.

Report Heading

The report heading displays the name of the report, the date that the report was run, and the page number.

Column Headings

User Name

The Oracle E-Business Suite name of the currently active user. The start and end dates that you specify in the Users window determine whether a user name is currently active.

Application Name

The name of the application associated with the responsibility.

Responsibility Name

The name of the currently active responsibility.

Start Date

The date when the user can begin accessing the responsibility. You can specify a start date when you assign the responsibility to the user in the Responsibilities block of the Users window.

End Date

The date when the user can no longer access the responsibility. You specify an end date when you assign the responsibility to the user in Responsibilities block of the Users window.

Disable and Enable Inactive FND Users Based on Security User Type

The Disable Inactive FND Users and Enable Inactive FND Users concurrent programs are enhanced in Oracle E-Business Suite Release 12.2.13 to consider the security user type in determining the user accounts they run against. These concurrent programs checks the value of a new profile option in Oracle E-Business Suite Release 12.2.13 called FND: Security User Type.

The profile option FND: Security User Type (FND_SEC_USER_TYPE) is valid for site and user levels and can be set to one of the following values:

- **NAMED** - Site level default or if the value is null.
- **SYSTEM** - System and internal account, exempt from inactive user locking policy.
- **PUBLIC** - Public account (GUEST), exempt from inactive user locking policy.

The Disable Inactive FND Users concurrent program checks the value of FND: Security User Type to determine which user accounts should be inactivated if they have not logged in within a specified amount of time and inactivates them.

Conversely, the Enable Inactive FND Users concurrent program allows for the re-activation of user accounts that were initially inactivated by the Disable Inactive FND Users concurrent program.

Reports and Sets by Responsibility Report

This report identifies which reports (and other concurrent programs) and report sets are

included in the request security groups available to any given responsibility. Use this report when defining or editing responsibilities.

Report Parameters

If you enter no parameters, the report documents all reports and report sets accessible from each responsibility.

Application Short Name

Choose the application name associated with the responsibility whose available reports and report sets you wish to report on.

If you do not choose an application name, the report documents all reports and report sets accessible from each responsibility.

Responsibility Name

Choose the name of a responsibility whose available reports and report sets you wish to report on. You must enter a value for Application Short Name before entering a value for Responsibility Name.

Report Headings

The report headings list the report parameters you specify, and provide you with general information about the contents of the report.

Related Topics

Overview of Oracle E-Business Suite Security, page 4-1

Defining Request Security, page 4-7

Responsibilities field help, page 4-22

Oracle Application Object Library REST Security Services

Oracle E-Business Suite Release 12.2 introduces Oracle Application Object Library *REpresentational State Transfer* (REST) security services as a new integration option, providing more versatility than previously possible. In particular, the REST security services facilitate the development of customizable support for mobile applications.

How these services are used is detailed under the descriptions of the four main APIs that are associated with them:

- Login Service
- Session Management Service

- Authorization Service
- Logout Service

Login Service

Every web service request made to Oracle E-Business Suite must be *authenticated*: that is to say, have the caller's credentials validated. The authentication process is often more informally referred to as *logging in*.

The REST Login Service validates the Oracle E-Business suite user credentials, and returns an access token. This access token can then be used with every subsequent service request that requires authentication, without the need for the user name and password to be sent every time.

The Login Service is based on the HTTP basic authentication scheme.

```
URL:
  http(s):://<EBSHost>:<EBSPort>/OA_HTML/RF.jsp?function_id=mLogin

HTTP Methods
  GET or POST

Content Type:
  JSON, XML

HTTP Headers:
  Authorization header as per HTTP BASIC authentication scheme
  Accept-Language header for client language in RFC 5646 format.
  Input Parameters:
    No input payload
 Output Parameters:
     accessToken - Token to be passed with every service request
requiring authentication
   accessTokenName - Name of the access token
   ebsVersion - Oracle E-Business Suite release version
   userName - Authenticated Oracle E-business Suite user name

Sample Request:

  GET /OA_HTML/RF.jsp?function_id=mLogin HTTP/1.1
  Authorization: Basic c3lzYWRtaW46c3lzYWRtaW4=
  Accept-Language: en-GB,en-US;q=0.8,en;q=0.6
  Content-Type: application/xml

Sample possible responses:

  200 (On Success):

  <response>
    <data>
      <accessToken>xxxxxxxxxxxxxxxxxxxxxxxxxx</accessToken>
      <accessTokenName>example</accessTokenName>
      <ebsVersion>12.2.0</ebsVersion>
      <userName>SYSADMIN</userName>
    </data>
  </response>

  401 (On Failure)

  <response>
    <status>
      <code>401</code>
      <description>Invalid username/password</description>
    </status>
    <data>
      <accessToken>-1</accessToken>
      <accessTokenName></accessTokenName>
      <ebsVersion></ebsVersion>
      <userName></userName>
    </data>
  </response>
```

Session Management Service

Any operation or service processing Oracle E-Business Suite data (to read, insert, update, or delete) is sensitive to the Oracle E-Business Suite security context (responsibility, application, security group, and operating unit). This means that the same operation will have different results if performed with a different security context. It is therefore critical to maintain a meaningful security context for the relevant

requests, and to reset this security context when required.

The Session Management REST service allows the client to initialize and re-initialize the Oracle E-Business Suite session's security context at any time. This service upgrades the access token with the security context information, so that all the requests holding the access token implicitly carry the security context information to the service provider.

The Session Management REST service also retrieves the current session security context information when required.

```
URL:
  http(s):://<EBSHost>:<EBSPort>/OA_HTML/RF.jsp?function_id=mInit

Content Type:
  JSON, XML

HTTP Headers:
  Cookie header with accessTokenName and accessToken from mLogin Service

Operation 1:
  To retrieve current session context information

HTTP Method:
  GET

Input Parameters:
  No input payload

Output Parameters:
    "resp" - responsibility information in the following structure
     id - responsibility ID
     applId - responsibility application id
     key  - responsibility internal name
     applKey - responsibility application short name
    "securityGroup" - Security group information in the following
structure
     id - Security group ID
     key - security group internal name
    "org" - Operating Unit information in the following structure
     id - Operating Unit id
     key - Operating unit internal name
    "userId" - authenticated Oracle E-Business Suite user ID
    "username" - authenticated Oracle E-Business Suite user name
    "accessToken" - current access token
    "accessTokenName" - current access token name
    "language" - Current session language

Sample Request:

  GET /OA_HTML/RF.jsp?function_id=mInit HTTP/1.1
  Cookie: <accessTokenName>=<accessToken>
  Content-Type: application/xml

Sample Possible Responses:

  200 (On Success):

  <response>
    <data>
      <resp>
        <id>20872</id>
        <key>SYSTEM_ADMINISTRATION</key>
        <applId>178</applId>
        <applKey>ICX</applKey>
      </resp>
      <securityGroup>
        <id>0</id>
        <key>STANDARD</key>
      </securityGroup>
      <org>
        <id>1733</id>
        <key>Vision Communications (USA)</key>
      </org>
      <userId>0</userId>
      <userName>SYSADMIN</userName>
      <accessToken>xxxxxxxxxxxxxxxxxxxxxxxxxxx</accessToken>
```

```
<accessTokenName>example</accessTokenName>
    <language>US</language>
    </data>
  </response>

'On Failure' returns the following HTTP error status codes along with
error description based on different error
conditions. Besides this information in response body the service also
returns the corresponding HTTP error status
code:

400 - for any invalid input payload
500 - for any unexpected exceptional conditions, which should be a code
bug
401 - for unauthorized access

Sample failure response:

  <response>
    <status>
      <code>error status code</code>
      <description>error description</description>
    </status>
    <data></data>
  </response>


Operation 2:

To initialize or re-initialize the Oracle E-Business Suite session's
security context

HTTP Method:
  POST

Input Parameters:
  "resp" - responsibility information in the following structure:
      id - responsibility ID
      applId - responsibility application ID
      key - responsibility internal name
      applKey - responsibility application short name
        o Supports both IDs and keys (internal names).
        o Uses either id attributes or key (internal name) attributes
for passing responsibility information.
        o A combination of id attribute for one entity and key attribute
for another entity is not supported. For example,
          id (responsibility id), applKey is NOT supported. Similarly,
appId (responsibility application ID), key
          (responsibility internal name) is not supported.
      "securityGroup"  - Security group information in the following
structure. Supports both IDs and keys (internal names). Use
       either id attribute or internal key attribute for passing
security group information.
       o id -  Security group ID
       o key - Security group internal name
      "org" - Operating Unit information in the following structure. It
supports both the ID and key (internal name). Use either ID
      attributes or internal key attribute for passing operating unit
information.
       o id - Operating Unit ID
       o key - Operating unit internal name

The parameters "resp", "securityGroup", and "org" are all optional.
The  request must send at least one of the parameters (rest,
securityGroup, org)
All the input parameters are case sensitive
```

```
Output Parameters:

Status Response

Sample Request:

  POST /OA_HTML/RF.jsp?function_id=mInit HTTP/1.1
  Cookie: <accessTokenName>=<accessToken>
  Content-Type:application/xml

    <data>
      <resp>
        <key>SYSTEM_ADMINISTRATION</key>
        <applKey>ICX</applKey>
      </resp>
      <securityGroup>
        <key>STANDARD</key>
      </securityGroup>
      <org>
        <key>Vision Communications (USA)</key>
      </org>
    </data>

Sample Response:

200 (On Success):

  <response>
    <status>
      <code>200</code>
      <description>success</description>
    </status>
    <data></data>
  </response>

'On Failure' returns the following HTTP error status codes along with
error description based on different error
conditions. Besides this information in response body, the service also
returns the corresponding HTTP error status
code:

400 - for any invalid input payload
500 - for any unexpected exceptional conditions, which should be a code
bug
401 - for unauthorized access

Sample failure response:

<response>
  <status>
    <code>error status code</code>
    <description>error description</description>
  </status>
  <data></data>
</response>
```

Authorization Service

This Oracle Applications Object Library REST security service allows client applications to retrieve the list of the assigned responsibilities, roles, and privileges for all logged-in users, filtered by specified criteria. The authorization security data returned by the service works with both with traditional function security and the RBAC model.

```
URL:
  http(s):://<EBSHost>:<EBSPort>/OA_HTML/RF.jsp?function_id=mACS

HTTP Method:
  POST

Content Type:
  JSON

HTTP Headers:

  Cookie header with accessTokenName and accessToken from mLogin Service

Operation 1

  Returns logged-in user's roles and responsibilities filtered by input
filter criteria.

  Input Parameters:

  "mode" - Honors values {"role", "resp", "roleresp", "parent"}. When
the value is:
      "role":  The service returns all the logged-in user's roles
matching the filter criteria.
      "resp": The service returns all the logged-in user's
responsibilities matching the filter criteria
      "roleresp": The service returns the logged-in user's both the
roles and responsibilities matching the
       filter criteria
      "parent": For all the roles/responsibilities matching the filter
criteria, this service returns the
       assigning role (wf_user_role_assignments.assigning_role). The
assigning role may be different than the
       immediate parent in the role hierarchy.
   "appName" - Application Short Name. To filter the authorization data
based on application short name.
   "roleCode" - Internal name of role/responsibility (WF_LOCAL_ROLES.
NAME). To filter the authorization data based
    on internal name of role/responsibility

Output Parameters:

  "data" - The array of roles/responsibilities in the following
structure.
      "NAME" - Internal name of role/responsibility
      "DISPLAY_NAME" - Display name of role/responsibility in session
language
      "RESPONSIBILITY_ID" - WF Orig_System_Id for a role and
responsibility ID for a responsibility
      "RESPONSIBILITY_APPLICATION_ID" - owning application ID of a
role/responsibility
      "APPL_SHRT_NAME" - Owning application short name of a
role/responsibility
      "SECURITY_GROUP_KEY" - Security group internal name for a
responsibility.

Sample Request:

  POST /OA_HTML/RF.jsp?function_id=mACS HTTP/1.1
  Cookie: <accessTokenName>=<accessToken>
  Content-type:application/json

   {
     mode:"role",
     appName:"FND",
     roleCode:"UMX|FND_SYSTEM%"
```

```
}
```

Sample Response:


```
  "data":[{
  "NAME":"UMX|FND_SYSTEM_INTEGRATION_DEVELOPER",
  "DISPLAY_NAME":"System Integration Developer",
  "RESPONSIBILITY_ID":"0",
  "RESPONSIBILITY_APPLICATION_ID":"0",
  "APPL_SHRT_NAME":"FND",
  "SECURITY_GROUP_KEY":"NONE"
},{
  "NAME":"UMX|FND_SYSTEM_INTEGRATION_ANALYST",
  "DISPLAY_NAME":"System Integration Analyst",
  "RESPONSIBILITY_ID":"0",
  "RESPONSIBILITY_APPLICATION_ID":"0",
  "APPL_SHRT_NAME":"FND",
  "SECURITY_GROUP_KEY":"NONE"
}]
```


On Failure returns the following HTTP error status codes, along with error description based on different error conditions. Besides this information in response body, the service also returns the corresponding HTTP error status code:

400 - for any invalid input payload
500 - for any unexpected exceptional conditions, which should be a code bug
401 - for unauthorized access

Sample failure response:


```
  {
    "status":{
    "code":"401",
    "description":"This is a bad request"
  }
```


Operation 2

Returns logged-in user's privileges (EBS executable functions and non-executable permissions), filtered by input filter criteria.

Input Parameters:

"mode" - Honors only value {"function"}. When the value is:
"function": the service returns all the logged-in user's privileges matching the filter criteria.
"resp" - array of responsibilities (with the below structure of attributes) for which accessible privileges is retrieved
"resp_id" - responsibility Id
"appl_id" - responsibility_application_id
"secgrp_id" - security_group_id
"filter" - An optional filter criteria at "resp" record level to filter the list of accessible privileges from this responsibility.
o "functionName" - Function internal code based on which list of accessible privileges from this responsibility are filtered.
o "webCall" - EBS Function FND_FORM_FUNCTIONS.WEB_HTML_CALL based on which list of accessible privileges from this responsibility are filtered

```
"filter" - Global filter criteria applied on all the accessible
privileges retrieved from the list of all
     input responsibilities. Global filter criteria is being over-ridden
by the resp specific filter criteria (if
     provided) for it's accessible privileges.
      o "functionName" - Function internal code based on which list of
accessible privileges from the entire
          responsibility list are filtered
      o "webCall" - EBS Function FND_FORM_FUNCTIONS.WEB_HTML_CALL based
on which list of accessible privileges from
         the entire responsibility list are filtered.

Output Parameters:

  "data" - The array of responsibilities along with the corresponding
privileges list in the following structure.
      "resp_id" : Responsibility Id
      "appl_id" : Responsibility Application Id
      "secgrp_id"  : Security Group Id
      "responsibility_name" : Responsibility Display Name
      "funcDetail" : Array of privileges accessible from this
responsibility. The privilege has the following structure:
       "RESPONSIBILITY_NAME" : Responsibility display name
       "FUNCTION_ID" : Function Id
       "FUNCTION_NAME" : Internal Function Name
       "USER_FUNCTION_NAME" : Function display name
       "WEB_HTML_CALL" : For executable functions, the function URL

Sample Request:

  POST /OA_HTML/RF.jsp?function_id=mACS HTTP/1.1
  Cookie: <accessTokenName>=<accessToken>
  Content-type:application/json

    {
      mode:"function",
      resp:[
            { resp_id:20420, appl_id:1, secgrp_id:0,
              filter: {functionName:"%HELP%"}
            },
          { resp_id:23175, appl_id:861, secgrp_id:0
            }
           ],
      filter: {
        functionName:"%HELP%",
        webCall:"%"
       }
    }

Sample Response:

  {
  data:
    {
     resp_id: "20420"
     appl_id: "1"
     secgrp_id: "0"
     responsibility_name: "System Administrator"
     funcDetails:
      {
       function_id: "1002781"
       function_name: "FND_HELP_BUILDER"
       user_function_name: "Help Builder"
       web_html_call: "jsp/fnd/fndhelpbuilder.jsp?custom_level=10"
      }
      {
```

function_id: "1035387"
       function_name: "FND_HELP_REPORTS_PAGE"
       user_function_name: "Fnd Help Reports Page"
       web_html_call: "OA.jsp?
page=/oracle/apps/fnd/gfm/webui/FndHelpReportsPG"
      }
    }
    {
     resp_id: "23175"
     appl_id: "861"
     secgrp_id: "0"
     responsibility_name: "iMeeting System Monitor responsibility"
     funcDetails:
      {
       function_id: "1005377"
       function_name: "ICX_HELP"
       user_function_name: "Self Service Help"
       web_html_call: "fndgfm/fnd_help.get/US/FND/@ICXPHP"
      }
      {
       function_id: "1032936"
       function_name: "UMX_LOGIN_HELP"
       user_function_name: "Login Help UI"
       web_html_call: "OA.jsp?
page=/oracle/apps/fnd/umx/password/webui/LoginHelpPG&akRegionApplication
Id=0"
      }
    }
  }

On Failure returns the following HTTP error status codes, along with error description based on different error conditions. Besides this information in response body, the service also returns the corresponding HTTP error status code:

400 - for any invalid input payload
500 - for any unexpected exceptional conditions, which should be a code bug
401 - for unauthorized access

Sample failure response:

  {
  "status":{
  "code":"401",
  "description":"This is a bad request"
  }

Operation 3 - Oracle E-Business suite implementation for ADFmf ACS interface)
Provides an Oracle E-Business Suite implementation for ADFmf pre-defined interface for ACS REST service.

Input Parameters:
  "userId" : Logged-in EBS username. If this differs from logged-in user, it reports an error.
  "filterMask" : Array honoring values {role, privilege}. When the value is :
     "role" : Filters the data based on roles passed through roleFilter
     "privilege" : Filters the data based on privileges passed through privilegeFilter
  "roleFilter" : List of role and responsibility internal codes (WF_LOCAL_ROLES.NAME) on which data is filtered.
  "privilegeFilter"": List of functions and internal codes (FND_FORM_FUNCTIONS.FUNCTION_NAME) on which data is filtered.

```
Output Parameters:
  "userId"   : logged-in Oracle E-Business Suite user name.
  "roles"   : List of logged-in user roles and responsibilities in
internal codes
  "privileges"    : List of logged-in user functions in internal codes

Sample Request:

  POST /OA_HTML/RF.jsp?function_id=mACS HTTP/1.1
  Cookie: <accessTokenName>=<accessToken>
  Content-type:application/json

    {
    "userId": "johnsmith",
    "filterMask": ["role", "privilege"],
    "roleFilter": [ "role1", "role2" ],
    "privilegeFilter": ["priv1", "priv2", "priv3"]
   }

Sample Response:

  {
    "userId": "johnsmith",
    "roles": [ "role1" ],
    "privileges": ["priv1", "priv3"]
  }
```

Logout Service

Logout Service invalidates the access token as an authentication mechanism, and thereby also invalidates any associated authenticated sessions.

```
URL:
 /OA_HTML/RF.jsp?function_id=mLogout

HTTP Methods:
  GET

Content-Type:
  XML or JSON

HTTP Headers:
  Cookie header with accessTokenName and accessToken from mLogin Service

Input Parameters:
 No input parameters

Output parameters :
  "accessToken" : Invalidated access token

Sample Request:

  GET /OA_HTML/RF.jsp?function_id=mLogout HTTP/1.1
  Cookie: <accessTokenName>=<accessToken>
  Content-type:application/xml

Sample Response:

  <response>
    <data>
      <accessToken>-1</accessToken>
      <accessTokenName>example</accessTokenName>
      <ebsVersion />
    </data>
  </response>

'On Failure' returns the following HTTP status codes along with error
description based on different error conditions:

500 - for any unexpected exceptional conditions

  <response>
    <status>
  <code>500</code>
  <description>Detailed error description</description>
    </status>
    <data></data>
  </response>
```

Cookie Domain Scoping

A *cookie* is a mechanism of storing state information across requests to a website. When a site is accessed, a user's browser uses the cookie to store information such as a session identifier. When the site is accessed on a future occasion, the information in the cookie can be reused.

If a domain is not specified, the browser does not send the cookie beyond the originating host. Explicitly setting the cookie domain scope tells the browser where the cookie can be sent.

Features of Cookie Domain Scoping include:

- Reduces the attack surface of Oracle E-Business Suite

- Provides additional protection for communication between the browser and the Oracle E-Business Suite web tier
- Provides the ability to define the scope for cookie sharing to avoid unnecessary exposure
- Allows for a custom scope to be defined

Cookie domain scoping configuration is set using the profile option "Oracle Applications Session Cookie Domain" (ICX_SESSION_COOKIE_DOMAIN).

By default, Oracle E-Business Suite will set the cookie domain attribute to the domain name of your site in order to ease integration of "external" integrations such as Discoverer, Kanban, and Single Sign-On. If you do not require the session cookie domain to be set because of "external" integrations such as Discoverer, you can set the ICX session cookie to be sent back on to the Oracle E-Business Suite web entry point.

> **Additional Information:** Concerning Oracle Discoverer, see My Oracle Support Knowledge Document 2277369.1, *Oracle E-Business Suite Support Implications for Discoverer 11gR1*.

The ICX_SESSION_COOKIE_DOMAIN profile option can take the following values:

- **Host**: (Recommended value) The domain attribute of the cookie will not be set. The cookie is scoped (restricted) to the originating server, and not sent to any other machines. This setting offers the minimum possible attack surface, and therefore the maximum level of protection. It should always be the setting used in a DMZ environment.

  Example:

  ```
  host=myebsserver.us.example.com
  ICX_SESSION_COOKIE_DOMAIN=HOST
  Set-Cookie: <no domain attribute>
  ```

- **Domain**: The domain attribute of the cookie will be set. The cookie is shared with all hosts in first level domain, with the domain value being derived from the APPS_WEB_AGENT profile option. This setting is the default, and is similar to pre-12.2 behavior.

  Example:

  ```
  host=myebsserver.us.example.com
  ICX_SESSION_COOKIE_DOMAIN=DOMAIN
  Set-Cookie: ...; domain=.us.example.com
  ```

- **Custom**: The domain value is user-defined. A broader scope for the cookie may be specified. This setting is not generally recommended.

  Example:

```
host=myebsserver.us.example.com
ICX_SESSION_COOKIE_DOMAIN=.example.com (CUSTOM)
Set-Cookie: ...; domain=.example.com
```

Implementing Cookie Domain Scoping

When setting up this feature, you should take into account the following:

- Identify any integrations that use an Oracle E-Business Suite cookie and determine what domains these cover.
- Scope cookies to narrowest domain consistent with business or other operational requirements.
- Always scope DMZ cookies to Host setting.
- Aim to use narrow cookie scoping when planning new configurations.

Troubleshooting Cookie Domain Scoping

Problem: Authenticated Oracle E-Business Suite users cannot navigate to external integrations such as Oracle E-Business Suite Information Discovery.

Check the following:

- The value of the ICX_SESSION_COOKIE_DOMAIN profile at site and server levels.
- Domains of the Oracle E-Business Suite and external integrations with which browser is communicating.
- Response headers containing `Set-Cookie`. The easiest method to do so is to use your browser's developer tools. Alternatives are intercepting proxy (more difficult with TLS enabled) and Apache logging.

Problem: When setting the domain, browser is not sending cookie back to host.

Check the following:

- Ensure that the APPS_WEB_AGENT profile option matches the web entry point with which the browser is communicating.

Problem: With a custom setting, browser is not sending cookie back to host.

Check the following:

- Custom value must be a strict subset of host name. For example, the browser will not send a cookie with a domain of `domain.example.com` to `otherdomain.example.com`.

Problem: With a custom setting, browser is not sending cookie to a host in another registerable domain.

Check the following:

- Check that the custom value corresponds to a registerable domain such as `example.com` and not a non-registerable domain such as `.com`. Browsers do not allow cookies to be shared or scoped across different registrable domains. For example, it is not possible to share cookies between `example.com` to `example.net`.

References

For more information, see My Oracle Support Knowledge Document 1375670.1, *Oracle E-Business Suite Release 12.2 Configuration in a DMZ*.

Allowed Resources

Introduction

The *Allowed Resources* feature reduces the attack surface of Oracle E-Business Suite by enabling the creation of an allowlist of resources - JavaServer Pages (JSPs) and servlets - that are permitted to be accessed in your environment. This feature adds additional protected resources (such as servlets) to the former Allowed JSPs feature which existed in previous versions of Oracle E-Business Suite Release 12.2. Configuration of actively allowed resources avoids unnecessary exposure, with unused resources being denied access.

> **Note:** An *allowlist* is a list of items that are explicitly granted access to a resource.

All Oracle E-Business Suite resources (JSPs and servlets) are predefined for you in the Allowed Resources feature. The implementation strategy also allows custom resources to be defined in the list of allowed resources.

The Allowed Resources feature offers multiple levels of protection. You can deny Oracle E-Business Suite resources using the options to manage by product family, products or resources. Using the feature with the shipped configuration provides some level of protection for minimal effort.

It is recommended that you start by disabling all Oracle E-Business Suite products that are not used in your environment. You can then add additional Oracle E-Business Suite resources and add your custom resources to match your family and product usage. This level of configuration is recommended for the best reduction in attack surface. You should also periodically refine and disable specific Oracle E-Business Suite resources.

> **Tip:** Conceptually, the principles are broadly similar to those employed in DMZs, which use a URL firewall as an allowlist mechanism. See My

Oracle Support Knowledge Document 1375670.1, *Oracle E-Business Suite Release 12.2 Configuration in a DMZ*.

More information regarding the steps to use Allowed Resources is provided in the following sections.

Allowed Resources is delivered and enabled by default (or "turned on") with Oracle E-Business Suite Release 12.2.7 or R12.ATG_PF.C.Delta.7.

The feature is also delivered through the October 2020 Critical Patch Update (CPU) for Oracle E-Business Suite Release 12.2.6 and earlier releases. After applying the CPU patch, you must manually enable the Allowed Resources feature. For more information about the latest CPU, see My Oracle Support Knowledge Document 2484000.1, *Identifying the Latest Critical Patch Update for Oracle E-Business Suite Release 12*.

Even if the Allowed Resources feature was previously enabled, when the October 2020 CPU is applied, the following products are turned off by default:

Products Turned Off by Default After Applying the October 2020 CPU

Product Group	Product Name	Product Short Code
Product Lifecycle Management	Oracle Document Management and Collaboration	DOM
Marketing & Sales	Oracle Marketing	AMS
Marketing & Sales	Oracle TeleSales	AST
Marketing & Sales	Oracle Sales for Handhelds	ASP
Marketing & Sales	Oracle Partner Management	PV
Marketing & Sales	Trade Management	OZF
Interaction Center	Oracle Advanced Outbound Telephony	IEC
Business Intelligence System	Oracle Business Intelligence System	BIS
Business Intelligence System	Oracle Balanced Scorecard	BSC

Product Group	Product Name	Product Short Code
Service Suite	Field Service Wireless	CSF

These products can be turned back on using the "Management by Product Hierarchy" page of the Allowed Resources feature.

How to Use Allowed Resources

The following outlines the strategy for using the Allowed Resources feature:

1. **Enable Allowed Resources.**

   Allowed Resources is delivered and enabled by default (or "turned on") with Oracle E-Business Suite Release 12.2.7 or R12.ATG_PF.C.Delta.7.

   If you are running R12.ATG_PF.C.Delta.6 or earlier, it is highly recommended that you upgrade to the latest ATG product family release as soon as possible. In the interim, see: Profile Options For Allowed Resources, page 4-85 to enable the feature.

   > **Note:** In order to enable or disable the Allowed Resources feature, you must bounce the WebLogic Server oacore managed server.

2. **Identify and deny access to Oracle E-Business Suite products that are not used in your environment.**

   Each Oracle E-Business Suite installation includes all products by default. An effective and easy way to reduce your attack surface using the Allowed Resources feature is to disable all Oracle E-Business Suite products that are not in use in your environment. To disable an Oracle E-Business Suite product is simple and only requires knowledge of the product families used by your company.

   To deny access to an Oracle E-Business Suite product, use the Management by Product Hierarchy page to review the filtered data and deny resources at the product or product family level that you know are not used (see: Management by Product Hierarchy, page 4-88).

3. **Add custom resources.**

   Allow access to identified custom resources. Use the All Resources tile on the Management by Resource page to individually add custom resources (see Management by Resource, page 4-92). Alternatively, you can add custom resources in bulk as described in Loading Customizations, page 4-99.

4. **Populate usage data.**

For a more accurate evaluation of the resources you should allow, it is ideal to collect at least one year's worth of access usage data. Data collection begins after the Allowed Resources feature is enabled, or once R12.ATG_PF.C.Delta.7 is applied. Data collection will stop if you disable the Allowed Resources feature and resumes when the feature is re-enabled.

You can optionally populate usage data from your Apache access logs by using the `webusage.awk` script and `WLDataMigration` utility described in Migration of Access Usage Data and Custom Resources, page 4-96.

5. **Identify and deny access to specific resources based upon usage.**

   Note: For this step, you must collect usage data as described previously in Step 4.

   Once a sufficient amount of access usage data is collected for the system, use the Management by Resource page to deny access to resources which have never been used or are no longer in use (see: Management by Resource, page 4-92). Oracle recommends this is done after 13 months of data has been collected. The start date of data collection is listed on the upper left of the Management by Resource page.

6. **Continue to improve the list of resources.** *(ongoing)*

   Periodically review the usage data and modify the configuration as needed, especially when deployment of new features or products occur, or products or features are no longer used.

Profile Options For Allowed Resources

As of Oracle E-Business Suite Release 12.2.11, there are two profile options used to configure the Allowed Resources feature: "Security: Allowed Resources" and "FND: Security Resource Logging".

Security: Allowed Resources and FND: Security Resource Logging

Profile Option Name	Code (Internal Name)	Recommended Value
Security: Allowed Resources	FND_SEC_ALLOWED_RESOURCES	CONFIG
FND: Security Resource Logging	FND_SEC_LOG_RESOURCES	UNRECOGNIZED

Security: Allowed Resources

The Allowed Resources feature is controlled by the profile Security: Allowed Resources (FND_SEC_ALLOWED_RESOURCES). The values for this profile option are as follows:

- **CONFIG**: Short for "configured," CONFIG is the profile option's default value in R12.ATG_PF.C.Delta.7 or Oracle E-Business Suite Release 12.2.7 and later. This value enables the Allowed Resources feature.

- **ALL**: Setting the profile option to ALL, meaning all resources are allowed, will disable the Allowed Resources feature. In releases prior to R12.ATG_PF.C.Delta.7 or Oracle E-Business Suite Release 12.2.7, where delivered by the CPU, this is the default.

  Note: Security: Allowed Resources will override the profile option Allow Unrestricted JSP Access (FND_SEC_ALLOW_JSP_UNRESTRICTED_ACCESS) delivered with R12.ATG_PF.C.Delta.4 and R12.ATG_PF.C.Delta.5, which are included in Oracle E-Business Suite Release 12.2.4 and Release 12.2.5, respectively.

Key characteristics of the Security: Allowed Resources profile option are as follows:

- It can be set at either the site or server level.

- A value of ALL turns off the feature and allows unrestricted access to resources. We recommend that you set FND_SEC_ALLOWED_RESOURCES=ALL for diagnostic purposes only. The Allowed Resources feature should not be turned off on your production system.

When the Security: Allowed Resources profile option is set to CONFIG, the profile options FND: Security Resource Logging (FND_SEC_LOG_RESOURCES) can be set to configure logging options for dispatcher type REQUEST.

Note: In order to enable or disable the Allowed Resources feature, you must bounce the WebLogic Server oacore managed server.

FND: Security Resource Logging

Set the profile option FND: Security Resource Logging (FND_SEC_LOG_RESOURCES) to one the following values to log access to requests of dispatcher type REQUEST: NONE, UNRECOGNIZED, and ALL.

- **NONE**: Setting FND: Security Resource Logging to NONE means that no requests of dispatcher type REQUEST are logged.

- **UNRECOGNIZED**: This is the default value. When FND: Security Resource Logging is set to UNRECOGNIZED, requests of dispatcher type REQUEST are logged at the UNEXPECTED level where resources are either one of the following:
  - In the Allowed Resources metadata and disabled.
  - Not in the metadata and would be rejected if the Allowed Resources feature is enabled.
- **ALL**: Setting FND: Security Resource Logging to ALL logs all requests of dispatcher type REQUEST.

  Note: The values for the FND: Security Resource Logging profile option have been updated for Oracle E-Business Suite Release 12.2.11 and later. For reference, see FND: Security Resource Logging Profile Option Values for Earlier Releases, page H-1 in "Appendix H: Security Features for Earlier Oracle E-Business Suite Releases" for profile option values prior to Release 12.2.11.

When requests are REJECTED and logged, logs are produced in the detailed log format, described in Log Formats, page 4-87.

Requests that are ACCEPTED are logged as follows:

- If the profile option FND: Debug Log Level (AFLOG_LEVEL) is set to STATEMENT, logs are produced in the detailed format, as described in Log Formats, page 4-87.
- All others are logged in the simple log format, as described in Log Formats, page 4-87.

Log Formats

Logs that are produced as a result of the FND: Security Resource Logging profile option are either in a simple log format or detailed log format.

Simple Log Format

The simple log format is as follows:

```
Id [Type] [Action] [Method] [Source --> Destination] [Referer]
```

For example, a simple log entry could look like this:

```
1864 [REQUEST] [REJECTED] [GET]  ["" --> "/OA_HTML/index.jsp"]
["https://host.example.com:4443/OA_HTML/OA.
jsppage=/oracle/apps/icx/icatalog/shopping/webui/ShoppingHomePG&_ti=xxxx
xxxxxx&oapc=4&OAMC=xxxxxxx_xxx_0&menu=Y&oaMenuLevel=1&oas=xxxxxxxxxxxxxx
xxxxxxxx.."]
```

Detailed Log Format

The detailed log format is as follows:

```
Id [Type][Action][Method][Source --> Destination][Referer][Remote
Address][XSID][Username][SessionId][Stack]
```

For example, a detailed log entry could look like this:

```
43 [REQUEST][REJECTED] [GET] ["" --> "/OA_HTML/testRejected.jsp"] [""]
[10.76.52.228] [xxxxxxxxxxxxxxxxxxxxxxxxxx] ["SYSADMIN"] ["xxxxxxxxxx"]
[Stack: "[]"]
```

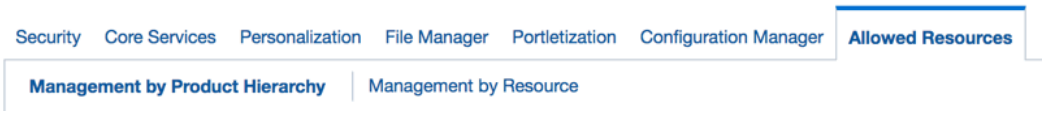
Allowed Resources Home Page

The Allowed Resources user interface (UI) makes it easier for administrators (specifically, Applications administrators) to configure the Allowed Resources feature by analyzing data usage and allowing or denying access to specific resources, configuring at a product family, product, or resource level. The Allowed Resources feature was introduced in Oracle E-Business Suite Release 12.2.7 and the UI has since been enhanced.

To access the Allowed Resources home page, select the Functional Administrator responsibility in the Navigator pane on the Oracle E-Business Suite home page. Then, on the Functional Administrator page, select the **Allowed Resources** tab.

Once within the Allowed Resources tab, there are two subtabs: **Management by Product Hierarchy** and **Management by Resource**.

Allowed Resources Tabs



An alternative method for accessing these two subtabs is through the OAM Security Dashboard. To do this, from the Navigator pane on the Oracle E-Business Suite home page, select the System Administrator responsibility, click on **Oracle Applications Manager**, and then click **OAM Security Dashboard**. On the dashboard are two links to the previously mentioned subtab pages.

Management by Product Hierarchy

Management by Product Hierarchy allows you to configure your allowed resources on the product family level. It is recommended that when you first begin to use the Allowed Resources feature, review this page keeping in mind the products that you use so that you can turn off (disable) the unused products at the family level.

> **Note:** You must wait until the cached data is refreshed before any changes go into effect.

- For R12.ATG_PF.C.Delta.7 or Oracle E-Business Suite Release 12.2.7 and later, the check frequency is automatically set to 60 seconds.

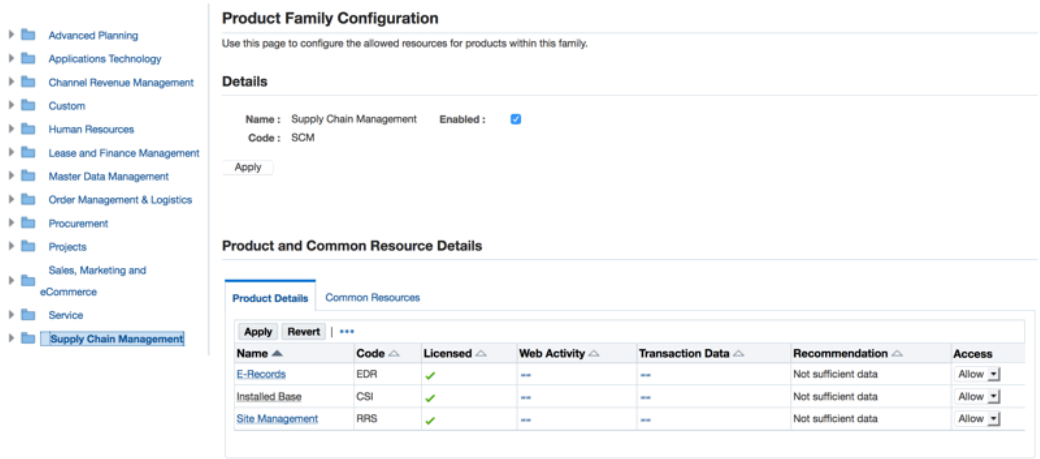
This check rate value cannot be changed.

- For prior versions of the ATG product family and Oracle E-Business Suite Release 12.2.6 and earlier, the UPDATE_CHECK_INTERVAL value is used to determine the refresh timing. The default value of UPDATE_CHECK_INTERVAL is 60 seconds.

On the Management by Product Hierarchy page, start by selecting a family name from the left menu to view the Product Family Configuration page for the selected product family.

From here, the Product Family Configuration page is divided into two main sections: Details and Product and Common Resource Details.

Product Family Configuration Page



The Details section displays basic information about the product family, such as the name and short code. The **Enabled** checkbox indicates whether or not the product family resources are allowed. Once the product family is enabled, you can add or remove individual products from the Allowed Resources allowlist. Select/deselect the checkbox and click **Apply** to implement changes.

Use the Product and Common Resource Details section of the page to configure products. This section is where you should focus your configuration efforts.

In the **Product Details** tab of this section, displayed is a table of products within the selected product family and important information about each product.

- **Code**: The product short code.
- **Licensed**: A green check mark or a red "X" indicates whether or not the product is licensed in License Manager.

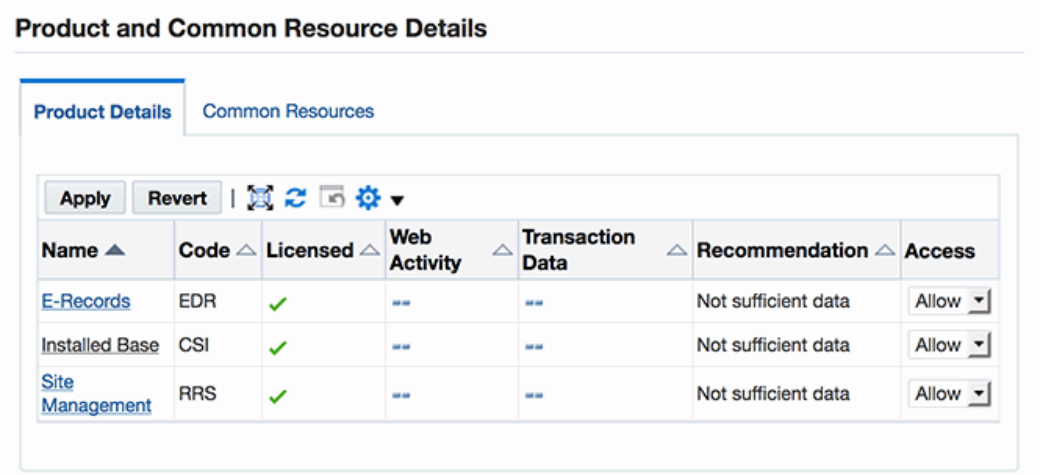
- **Web Activity**: This is at the product-level and indicates whether or not there has been any activity associated with the resources or by the resources within the product. For example, every time the resource is requested, it is being tracked. Over time, this will continue to provide more information about what resources are in active use.

- **Transaction Data**: Queries are run in the database to see if any transactions are detected for the particular product, generally within the last year.

- **Recommendation**: Oracle's recommendation, based upon the previous 3 columns: Licensed, Web Activity, and Transaction Data.

- **Access**: Use the drop-down list to allow or deny access to this product's resources. After making a selection, click **Apply** at the top of the table.

Product and Common Resource Details Section - Product Details Tab



Click on a product name in the table found on the **Product Details** tab. The Resource Details are displayed. Here you can also select or deselect the **Enabled** checkbox in order to deny or allow access to the product.

Configuring resources at the details level is a task you may want to perform when you have collected sufficient activity data to be sure of the specific resources that are used in your configuration.

Resource Details - Used Tab

Resource Details

Used | Owned

Apply | Revert

Name	Type	Application	Web Activity	Access
/OA_HTML/jsp/edr/EDRRuleXMLPublisherHandler.jsp	JSP	EDR	--	Allow for product
/OA_HTML/jsp/edr/FilePreview.jsp	JSP	EDR	--	Allow for product
/OA_HTML/jsp/edr/iSignPublisherHandler.jsp	JSP	EDR	--	Allow for product

When in the Product Configuration page, generally speaking, you will be working mostly within the **Used** tab of the Resource Details section. The resources listed in this tab are those that are exposed for the selected product. Change access to the resource by selecting either "Allow for product" or "Deny for product" in the drop-down list found in the Access column. This is another method for allowing/denying access to a product, in addition to enabling access in the Details section of the Product Family Configuration page.

The **Owned** tab in the Resource Details provides you with a listing of resources owned by this product and if any product is currently exposing that resource.

Resource Details Section - Owned Tab

Resource Details

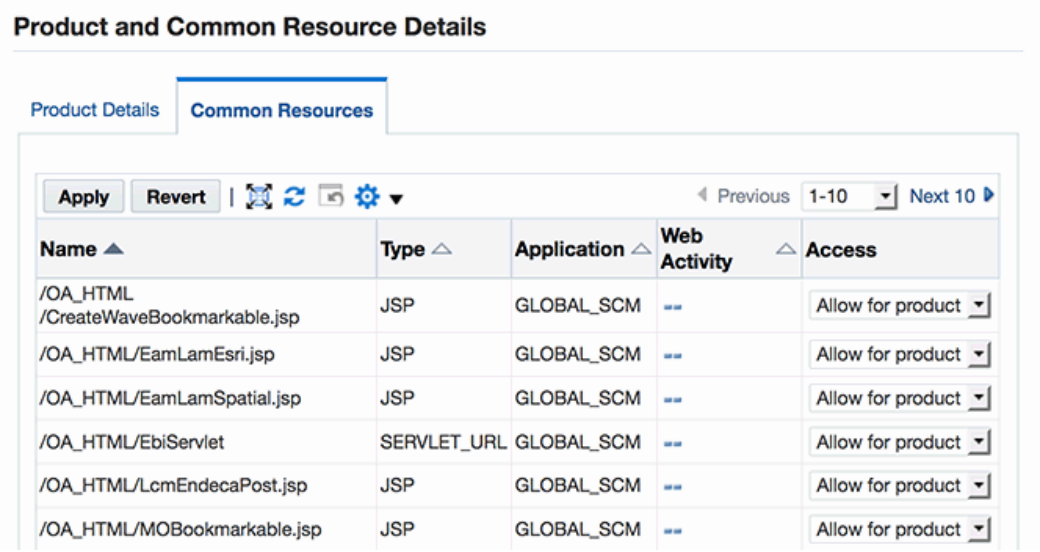
Used | Owned

Name	Type	Web Activity	Status
/OA_HTML/jsp/edr/EDRRuleXMLPublisherHandler.jsp	JSP	--	Used
/OA_HTML/jsp/edr/FilePreview.jsp	JSP	--	Used
/OA_HTML/jsp/edr/iSignPublisherHandler.jsp	JSP	--	Used

Going back to the Product and Common Resource Details section of the Product Family Configuration page, beside the **Product Details** tab is the **Common Resources** tab.

On the **Common Resources** tab, listed are the common resources for all products for a product family. You can view and control these resources by selecting "Allow for product" or "Deny for product" in the drop-down list in the Access column.

Product and Common Resource Details Section - Common Resources Tab



When it comes to allowing and denying access to resources on the Management by Product Hierarchy page, three levels of granularity exist:

- **At the Product Family Level**

  To allow and deny resources at the product family level, navigate to the Product Family Configuration page - Details section. Selecting the **Enabled** checkbox allows access to all product family resources; deselecting the **Enabled** checkbox denies the access.

- **At the Product Level**

  To allow and deny access at the product level, deny access to the appropriate product level on the **Product Details** tab in the Product and Common Resources section.

- **At the Resource Level**

  To view individual resources, you can drill down to the Resource Details in **Common Resources** tab. The Management by Resource page, discussed in the next section, provides a tailored interface for managing individual resources across the products that use the resource.

  > **Note:** In the event of problems, you should be prepared to revert modifications to family, product, or individual resources.

Management by Resource

Added in Oracle E-Business Suite Release 12.2.9 or after applying R12.ATG_PF.C.Delta.

8, the **Management by Resource** tab, allows you to evaluate your data usage. Six predefined filter criteria are displayed as tiles (previous versions utilize a combination of subtabs and saved searches). Prior to Oracle E-Business Suite Release 12.2.9 or R12. ATG_PF.C.Delta.8, the **Management by Resource** tab is delivered through the October 2020 CPU (see My Oracle Support Knowledge Document 2484000.1, *Identifying the Latest Critical Patch Update for Oracle E-Business Suite Release 12*, for more information).

The Management by Resource tiles are as follows:

- Allowed - But Never Accessed
- Allowed - Sorted by Last Access Date
- Allowed - Sorted by Access Count
- Allowed Resources
- Denied Resources
- All Resources

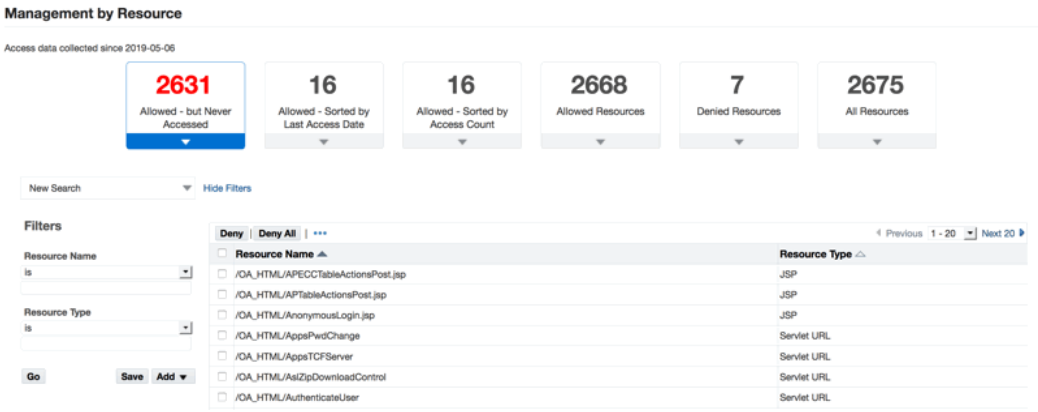
The "Access data collected since" date above the left most tile is the date in which the Allowed Resources feature was enabled and started collecting access usage data. Remember that for a more accurate evaluation of the resources you should allow, it is ideal to collect at least one year's worth of continuous access usage data. If you have access usage data from a previous environment, you can leverage the existing access logs by following the instructions in Migration of Access Usage Data and Custom Resources, page 4-96.

Click on each tile to view the filtered content in the table displayed. At the top of each table are buttons to allow or deny resources, as appropriate, or to perform further actions such as to show or hide columns. Note that not all columns are displayed by default.

You can further refine each tile's filters by utilizing the Filters section on the left. The Filter section allows you to add additional filter criteria and to save your search for later use. Saved searches are bound to a tile, therefore, each tile can have its own saved searches.

> **Note:** You must wait until the cached data is refreshed before the changes go into effect. The check frequency is automatically set to 60 seconds. This check rate value cannot be changed.

Management by Resource Page



Select the **Allowed - But Never Accessed** tile to view a listing of resources that are allowed but have not been accessed so that you can determine whether or not to deny access to these resources. Review this listing once sufficient access usage data has been collected.

- This listing can be filtered by Resource Name, Resource Type, and Owning Product.
- Click **Deny All** in order to deny all resources which have never been accessed. This will impact all resources in the query, and not just the resources currently displayed on the page. This can be reverted in the Denied Resources tile described later in this section. Before the action is complete, there will be a warning dialog box which tells how many resources will be denied.

  > **Note:** It is recommended that you do not deny all resources in this listing until a sufficient amount of usage data has been procured. Oracle recommends this is done after 13 months of data has been collected.

Select the **Allowed - Sorted by Last Access Date** and **Allowed - Sorted by Access Count** to view the resources that are currently allowed and accessed, listed by the most recent date of access and by the number of times that the resource has been accessed, respectively. The purpose of these tiles is to allow review of resources which have been used infrequently, or not used in a long time, since they may no longer require access.

- These listings can be filtered by Resource Name, Resource Type, Owning Product, Access Count, and by First or Last Access Date, depending on which tile is selected.
- Resources used infrequently or that have not been used in a long time can be evaluated to determine if access is required any longer. If no access is required, select the resource or resources, and click **Deny**.

Select the **Allowed Resources** tile to view all resources that are currently allowed.

- This listing can be filtered by Resource Name, Resource Type, Owning Product, Access Count, Creation Date, First Access Date, and Last Access Date.

- If a resource should not require access, but is found in this listing of allowed resources, select the resource or resources, and click **Deny**.

Select the **Denied Resources** tile to view resources that are currently denied.

- This listing can be filtered by Resource Name, Resource Type, Owning Product, Family Level Status, Product Level Status, Resource Level Status, First Access Date, Last Access Date, Access Count, and Denied Date.

- Denied resources from the other five tiles will shift to this listing.

- If you identify a resource in this listing that should require access, select the resource or resources, and click **Allow**. If all resources in the listing require access, click **Allow All**.

- If you wish to revert the resources that were denied on a specific date, filter the resources on "Denied Date" and use the **Allow All** function to allow those resources.

Select the **All Resources** tile to view all resources - This includes allowed, denied, accessed, and never accessed resources, as well as resources that are not associated with a specific product and therefore do not populate in any of the listings for the previous five tiles. The All Resources tile provides the ability to add or update a new or existing resource. You can also make changes to custom resources or change associated resources for a particular product or product family, such as changing the usage.

- This listing can be filtered by Resource Name, Resource Type, Owning Product, Creation Date, First Access Date, Last Access Date, or Access Count.

- The All Resources tile includes the resource type "Extension." The other tiles in Management by Resource UI do not include the extension resource type. Each tile also has specific default filters and search criteria. As a result of this, tile counts may not sum to the expected result. For example, the total count for "Allowed Resources" plus the total count of "Denied Resources" may not equal the total count for "All Resources."

- At the top of the table, click **Add** to add a custom resource. This opens the Add a Resource page. Provide a **Resource Name** and select a **Resource Type** from the provided drop-down list: extension, JSP, servlet pattern, servlet URL, or executable. Also, select an **Owning Product** from the drop-down list.

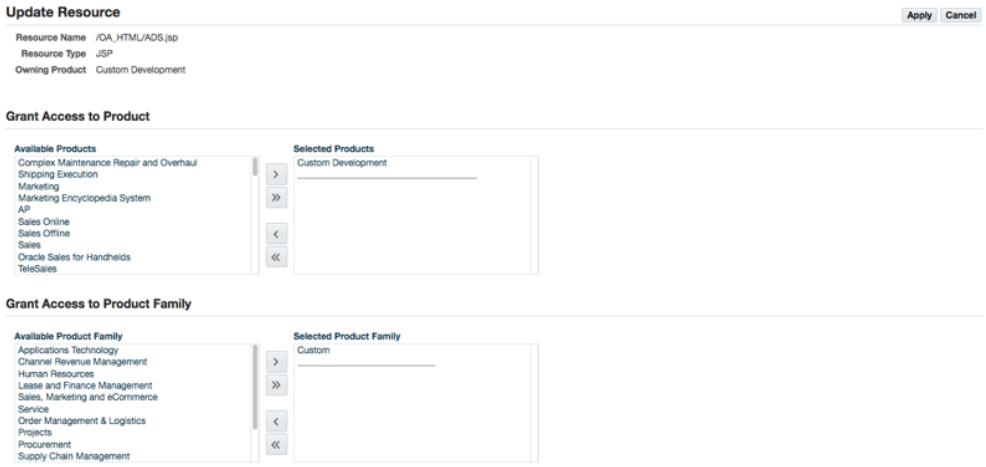
  > **Note:** If you are adding an extension resource, enter the extension as the **Resource Name**. For example, "spq" or "xsd."

After providing the resource details, grant the appropriate access to the resource at the product level or the product family level. Click **Apply** to submit the custom resource to the allowed resources repository.

If you wish to leverage your existing Apache access logs to identify custom resources and bulk upload them into the allowed resources repository, see Migration of Access Usage Data and Custom Resources, page 4-96.

- From within the table, you can click the pencil icon to update a specific resource, allowing or denying the resource access to certain products and product families.

Update Resource Page



Migration of Access Usage Data and Custom Resources

Tools

The following tools can be used to populate usage data and custom resources.

webusage.awk Script

The `webusage.awk` script is an awk script which can be used to generate a summary of resources used from any available Apache access logs. This can then be leveraged using the `WLDataMigration` utility to identify custom resources as well as to populate web usage data.

See My Oracle Support Knowledge Document 2069190.1, *Security Configuration and Auditing Scripts for Oracle E-Business Suite*, for the latest zip file containing the script.

WLDataMigration Command Line Utility

The `WLDataMigration` utility provides the ability to identify and populate custom resources and web usage data from your Apache access logs. It also allows you to

populate that information, or migrate existing custom resource configuration files in bulk, into the allowed resources repository.

You can access the `WLDataMigration` utility by using the following command line. Note that all parameters can, if desired, be entered on the same command line; they are shown here on different lines (using the UNIX "\" continuation character) for clarity.

```
java oracle.apps.fnd.security.resource.WLDataMigration \
MODE=<seed|custom> \
INPUT_FILE=<conf file/webusage file> \
DBC=<path of dbc> \
[PARSE_MODE=<single|recursive>]
```

The utility provides several different options:

- When `MODE=seed` and `INPUT_FILE` is a web usage file:
  - This mode allows you to leverage your existing Apache access logs to identify custom resources and associated usage data as well as to populate web usage data for existing allowed resource. It takes the `webusage.out` file as input which is generated using the `webusage.awk` script described in the previous section. This mode also produces a `CUSTOM.out` file of potential custom resources along with web usage data.

- When `MODE=custom` and `INPUT_FILE` is a web usage file:
  - The utility takes the `CUSTOM.out` file as input which was created as an output of the `MODE=seed` previously described. The `custom.out` file includes web usage data.

- When `MODE=custom` and `INPUT_FILE` is a simple configuration file:
  - The utility takes the `custom.conf` file as input from prior configuration of the Allowed Resources (or Allowed JSPs) feature. The `custom.conf` file does not include web usage data.

The `PARSE_MODE` parameter can also be added to the command. If `PARSE_MODE=single`, the `WLDataMigration` utility parses only individual resource entities in the configuration files. If `PARSE_MODE=recursive` searches for the "include" keyword and parses these included configuration files for resource data as well.

Migrating Access Usage Data

1. Download the `webusage.awk` script to summarize web usage activities from Apache access logs.

2. Run the `webusage.awk` script against your Apache access logs.

   A simple case where all relevant access_log files exist in one directory would be:

   ```
   $ cat access_log* | tr '?' ' ' | awk -f webusage.awk > webusage.out
   ```

The `webusage.out` may look something like this:

```
=============== WEB USAGE: 324512 lines, 1358 counted hits 2016-09-
11 - 2016-12-09
First hit seen   Most recent hit     #Hits URL
================ ================ ========
==============================
2016-11-08_19:38 2016-11-08_20:36        3
/OA_HTML/amsActMetricsHistLOV.jsp
2016-11-08_19:42 2016-11-08_19:42        1 /OA_HTML/amsApprFuncLOV.
jsp
...
2016-09-29_00:36 2016-12-08_18:06      308 /OA_HTMLAppsLocalLogin.
jsp
2016-11-04_20:27 2016-11-04_21:02        6 /OA_HTML/AppsLocalLogin.
jsp/%2e./jtffmeqq.jsp
...
2016-11-04_19:29 2016-11-04_19:31        5 /OA_HTML/cabo/jsps/a.jsp
2016-10-27_21:03 2016-11-08_00:08      195
/OA_HTML/cabo/jsps/frameRedirect.jsp
2016-09-11_11:12 2016-09-11_11:12        1 /OA_HTML/fake.jsp
```

To gather information about resources that have been used at your site, generate the `webusage.out` file as using the following command:

```
$ cd <location of the OHS access_log files>
$ cat access_log* | tr '?' ' ' | awk -f webusage.awk > webusage.out
```

Prior to running the above command, ensure all relevant access_log files are present in the location provided. Relevant access_log files will be those from the previous year or two.

For customers with multiple application tiers, copy the access_log.NNNNNNNNN files from each tier to a central location. If you have a limited log retention period in the runtime system and have archived older logs elsewhere, copy all access_log. NNNNNNNNN files to a central location.

If you have log files going back many years, you can limit the report to only include more recent entries by modifying the `access_log*` wildcard in the command.

Example wildcards are as shown:

```
access_log.14*       "May 13 16:53:20 UTC 2014"
access_log.14[789]*  "Jul 31 21:20:00 UTC 2016"
access_log.14[89]*   "Nov 24 15:06:40 UTC 2016"
access_log.15*       "Jul 14 02:40:00 UTC 2017"
```

In this example, to use all access logs after "Nov 24 15:06:40 UTC 2016," replace the wildcard `access_log*` with `access_log.14[89]* access_log.15* access_log` in the awk command line, as shown in the following command:

```
$ cat access_log.14[89]* access_log.15* access_log | tr '?' ' ' |
awk -f webusage.awk > webusage.out
```

3. Run the `WLDataMigration` utility to populate web usage data and generate the `CUSTOM.out` file (for resources that are not in the system). Use the following command:

```
$ java oracle.apps.fnd.security.resource.WLDataMigration MODE=seed
INPUT_FILE=webusage.out DBC=$FND_SECURE/<SID>.dbc
```

For example, the `CUSTOM.out` may look like this:

```
2016-09-11_11:12 2016-09-11_11:12        1 /OA_HTML/fake.jsp
2017-06-04_03:24 2017-06-14_03:27      538 /OA_HTML/CustLogin.jsp
```

Some of the resources listed in this file may be valid custom resources and some may be invalid requests. You should review and keep the resources that you want to add as custom resources.

Migrating and Loading Customizations in Bulk

Individual custom resources can be added through the All Resources tile of the Management by Resource page (see Management by Resource, page 4-92), although if you would like to load your custom resources in bulk, you can utilize the `webusage.awk` script and the `WLDataMigration` command. There are two methods for doing so:

- **Method 1**: Use the `CUSTOM.out` file, generated per the steps in Migrating Access Usage Data, page 4-97, to migrate existing custom resources discovered by the `webusage.awk` script run against your Apache access logs into the allowed resources repository. To invoke the `WLDataMigration` utility, use the following command:

  ```
  $ java oracle.apps.fnd.security.resource.WLDataMigration MODE=custom
  INPUT_FILE=CUSTOM.out DBC=$FND_SECURE/<SID>.dbc
  ```

  > **Note:** When using the `CUSTOM.out` file, review each entry to ensure that they are legitimate custom resources. For example, invalid results may have been caused by typos when editing the URL in the address bar or hits from a web scanner/penetration test (attempting to access non-existing resources).

- **Method 2**: You can use the `custom.conf` file as input from a prior configuration of the Allowed Resources (or Allowed JSPs) feature to migrate existing custom configuration files from your Apache access logs into the allowed resources repository.

  ```
  $ java oracle.apps.fnd.security.resource.WLDataMigration MODE=custom
  INPUT_FILE=custom.conf DBC=$FND_SECURE/<SID>.dbc
  ```

  Syntax for the `custom.conf` file is described in Loader File Syntax for Custom Resources in custom.conf, page 4-99.

Loader File Syntax for Custom Resources in custom.conf

Use the following syntax when making loader file customizations in the `custom.conf` file.

Loader File Syntax for JSPs

The following syntax is used in the loader files for JSPs:

- The full resource path must be specified for the underlying file associated with the allowed resource.

  Example:

  ```
  /OA_HTML/example.jsp
  ```

- Comments are denoted by a leading "#."

  Example:

  ```
  # This is a comment
  ```

Loader File Syntax for Servlets

The following syntax is used in the loader files to add custom servlet entries.

- If the servlet's URI mapping in the `web.xml` file has no trailing patterns, such as:

  ```
  /*--- web.xml ---*/
  <servlet-mapping>
   <servlet-name>AppsLogin</servlet-name>
   <url-pattern>AppsLogin</url-pattern>
  </servlet-mapping>
  ```

  List the servlet's URI pattern directly starting with `/OA_HTML`.

  For example:

  ```
  /*--- custom_servlets.conf ---*/
  # Sample entry for a servlet
  /OA_HTML/AppsLogin
  ```

- If the servlet's URI mapping in `web.xml` has a trailing wildcard (*) pattern, such as:

  For example:

  ```
  /*--- web.xml ---*/
  <servlet-mapping>
   <servlet-name>weboam</servlet-name>
   <url-pattern>/weboam/*</url-pattern>
  </servlet-mapping>
  ```

  List the servlet's resource pattern starting with `/OA_HTML` without the trailing wildcards with a "servlet" directive.

  For example:

  ```
  /*--- custom.conf ---*/
  # Sample entry with URL mapping that ends with *
  servlet /OA_HTML/weboam
  ```

  > **Note:** Starting with Oracle E-Business Suite Release 12.2.7, the pattern tag has been deprecated.

Logging and Troubleshooting

When this feature is enabled, you may find that access to required resources has been

blocked. In this case, you would get an HTTP 403 (Forbidden) response.

Seeing this message is the expected behavior (it is not an error) if it is seen on an attempt to access a resource that is intentionally restricted. On the other hand, it is an error (in that it should not be displayed) if it is seen on an attempt to access a resource that is unrestricted.

Logging can be used to investigate issues such as this. By default, it is disabled (turned off). When enabled, logging will write messages to the designated log file as follows:

- Whether or not the filter is enabled.
- Whether or not access is allowed to a resource on which an access attempt is being made.

Enabling Logging

Logging is enabled by setting the profile FND: Debug Log Enabled (AFLOG_ENABLED) to Yes and the log level to the appropriate level depending on the amount of information needed - Exception, Procedure, or Statement.

Common Issues

- *Symptom*: Error message denying access is displayed upon trying to access resource that should not be restricted.

  Probable Causes: (1) Resource is denied or not defined in the allowed resources repository. (2) Browser caching issue.

  Resolution: (1) Allow access to the resource or add the resources using the utility mentioned above. If you are on Oracle E-Business Suite Release 12.2.6 or earlier, uncomment the resource in configuration file or add the resource to configuration file. (2) Clear browser cache and restart browser.

- *Symptom*: Error message denying access is displayed upon trying to access resource that is on the list of allowed resources.

  Probable Causes: (1) URL does not match exactly. May be caused by double slashes in URLs, or different location. (2) Browser caching issue.

  Resolution: (1) Ensure the resource and location match exactly. (2) Clear browser cache and restart browser.

Allowed Redirects

Introduction

The *Allowed Redirects* security feature in Oracle E-Business Suite provides defense in-depth protection against phishing redirect attacks by enabling the configuration of

allowed redirects to avoid unnecessary exposure.

Similar to the Allowed Resources feature, Allowed Redirects restrict redirects by utilizing an allowlist mechanism, defining hosts with authorized access to a resource and denying access to those that are not in the allowed listing.

> **Note:** An *allowlist* is a list of items that are explicitly granted access to a resource.

Allowed Redirects is delivered with Oracle E-Business Suite Release 12.2.4 and later or R12.ATG_PF.C.Delta.4.

It is enabled by default (or "turned on") with Oracle E-Business Suite Release 12.2.6 later or with R12.ATG_PF.C.Delta.6 and later.

The feature is also delivered through the October 2020 Critical Patch Update (CPU) for Oracle E-Business Suite Release 12.2.5 and earlier releases. After applying the CPU patch, you must manually enable the Allowed Redirects feature. For more information about the latest CPU, see My Oracle Support Knowledge Document 2484000.1, *Identifying the Latest Critical Patch Update for Oracle E-Business Suite Release 12*.

It is important to note that this feature is specific to HTTP 302 redirects. It does not protect against other types of unrestricted redirects, such as a Java servlet forward or meta-refresh tags.

Getting Started

The basic strategy for deploying the Allowed Redirects feature is as follows.

1. Evaluate product family usage.
2. Cross-check restricted redirects against the access log.
3. Add custom redirects, as required.
4. Ensure the Allowed Redirects feature is enabled.
5. Continue to refine the allowlist. For example, comment out any redirects which do not seem to be used.

The main configuration file is: `$FND_TOP/secure/allowed_redirects.conf`.

Configuration Files

> **Note:** Apply the latest technology stack release update pack to receive the most current version of the configuration file. See My Oracle Support Knowledge Document 1617461.1, *Applying the Latest AD and TXK Release Update Packs to Oracle E-Business Suite Release 12.2*.

Syntax

The following syntax is used with the Allowed Redirects configuration file:

- Content listed should be hosts, domains, site or server level profiles, and/or additional configuration files.

- Comments are denoted by a leading '#'.

  Example:

  ```
  # domain example.com
  ```

- Include files may be defined.

  Example:

  ```
  include example_file.conf
  ```

Creating a Custom Configuration File

The procedure to do this is as follows:

1. Create a new custom configuration file. For example, `allowed_redirectsCUSTOM.conf`.

2. Add your customer redirect configurations to the custom configuration file. For example, host host1.example.com.

3. Add an entry in the `allowed_redirects.conf` file. For example, include `allowed_redirectsCUSTOM.conf`.

The `allowed_redirects.conf` file would then look something like this:

```
#--------------------------------------------
# Include Additional Config Files
# Add custom config files for custom redirects
#--------------------------------------------
# include <AllowedRedirectsCustom.conf>
include moreConfig.conf                 # in this same directory
include product/moreConfig.conf         # in a relative directory
include /somewhere/else/moreConfig.conf # in an absolute path
```

The following are configurations delivered in the configuration file:

- Oracle E-Business Suite built-in use of redirects for functionality

  Examples include: Report Launcher, Self-Service Applications, Help System

- Single sign-on integration with Oracle Access Manager using Oracle E-Business AccessGate and Oracle Directory Services

- Reporting with Oracle Discoverer Viewer, Oracle Discoverer Server and Oracle Business Intelligence Enterprise Edition

Additional Information: See also My Oracle Support Knowledge Document 2277369.1, *Oracle E-Business Suite Support Implications for Discoverer 11gR1*.

- Integration with Oracle Portal
- iRecruitment Background Check URL

Configurations which you may need to add to the configuration file based upon your environment:

- Oracle E-Business Suite iProcurement with Punchout (Add host or domain entry for each Punchout site), only for Releases 12.2 through 12.2.5

  Note: Starting with Release 12.2.6, configuration of allowed redirects for Oracle E-Business Suite iProcurement is performed automatically.

- Oracle E-Business Suite Configurator integration with Agile or Siebel using Oracle Application Integration Architecture (Add host or domain entry for each integration point)
- Any custom redirects used in your environment

Profile Options for Allowed Redirects

The profile option Allow Unrestricted Redirects (FND_SEC_ALLOW_UNRESTRICTED_REDIRECT) sets unrestricted or restricted access.

Key characteristics are:

- Can be set at the site or server level.
- As of Oracle E-Business Suite Release 12.2.6, the default value is No at the site level. This restricts access to the allowed redirects per the redirect allowlist filter.
- A value of Yes allows unrestricted redirects to occur. We recommend that you set FND_SEC_ALLOW_UNRESTRICTED_REDIRECT=Yes for diagnostic purposes only. This feature should not be turned off on your production system.
- A value of NULL enables restricted access if the redirect servlet filter is configured.
- This profile update requires a restart of the application tier services.

Allowing Redirects

There are three mechanisms for adding allowed redirects using the Allowed Redirects feature. Access can be added at the host, domain, and profile levels.

Example Host Configuration

```
#-------------------------------------------------------------------
# Allowed redirects configuration file
# Anything following a '#' is considered a comment
#-------------------------------------------------------------------
#----------------
# List of hosts
#----------------
# host target.example.com
...
```

Example Domain Configuration

```
...
#-------------------------------------------------------------------
# List of domains. This matches both host.internal.<DOMAIN_NAME>
# and host.external.<DOMAIN_NAME>
#-------------------------------------------------------------------
# domain example.com
...
```

Example Profile Configuration

```
#-------------------------------------------------------------------
# Server level profiles (site or server level)
#-------------------------------------------------------------------
profile APPS_SERVLET_AGENT              # URL for JSP and Servlets
profile APPS_FRAMEWORK_AGENT            # URL for Self Service
Applications entry point
profile APPS_AUTH_AGENT                 # URL for OAM and Access Gate
integration
profile APPS_SSO_POSTLOGOUT_HOME_URL    # URL to redirect on logout
profile ICX_DISCOVERER_VIEWER_LAUNCHER  # URL to launch Discoverer
Viewer
profile ICX_REPORT_LAUNCHER             # URL for Report Launcher
profile ICX_FORMS_LAUNCHER              # URL for the Forms Launcher
...
```

Additional Information: See also My Oracle Support Knowledge Document 2277369.1, *Oracle E-Business Suite Support Implications for Discoverer 11gR1*.

Testing Allowed Resources and Allowed Redirects

The following example can be used to test and understand the Allowed Redirects feature, as well as the Allowed Resources/JSPs feature. In this example, you will be adding in a custom JSP to the Allowed Resources allowlist, as well as allowing the system to redirect to a custom host.

Creating and Compiling the JSP

Place the following JSP code into a file called `redirectTest.jsp`:

```
<html>
<head>
   <title>Testing a redirect</title>
</head>

<body>
   <%
     String redirectURL = "https://example.org/wiki/HTTP_302";
     response.sendRedirect(redirectURL);
   %>
</body>
```

Now, compile:

```
[html]$ cp redirectTest.jsp $OA_HTML
[html]$ cd $OA_HTML
[html]$ $FND_TOP/patch/115/bin/ojspCompile.pl --compile -s
'redirectTest.jsp' -log err.log --flush
logfile set: err.log
starting...(compiling all)
using 10i internal ojsp ver: 10.3.6.0
quick compile:
  files to compile...1
translating and compiling:
  translating jsps...1/1 in 25s
  compiling jsps...1/1 in 3s
Finished!
```

As expected, the JSP redirects in Oracle E-Business Suite Release 12.1.3 and pre-12.2.6 instances where customers have not turned on the new features.

The JSP is not accessible when the Allowed Resources and servlets filter features have been turned on - these are turned on by default in Oracle E-Business Suite Release 12.2.6 and later. When the Allowed Resources feature is turned on, you will receive an HTTP 403 (Forbidden) response.

Adding a Custom Page to the Allowlist

```
[html]$ cd $FND_TOP/secure

vi $FND_TOP/secure/redirect_test_CUSTOM.conf
```

Add the following lines:

```
#Adding in for testing redirect filtering
/OA_HTML/redirectTest.jsp
```

Load the `redirect_test_CUSTOM.conf` into the database with the following command:

```
$ java oracle.apps.fnd.security.resource.WLDataMigration MODE=custom
INPUT_FILE=$FND_TOP/secure/redirect_test_CUSTOM.conf
DBC=$FND_SECURE/<SID>.dbc
...
Enter APPS username: APPS
Enter APPS password: ...
```

This JSP will now be enabled, you can disable it using the CUSTOM Family/Product in

the Allowed Resources user interface (UI).

You must wait until the cached data is refreshed before the changes go into effect.

- For R12.ATG_PF.C.Delta.7 or Oracle E-Business Suite Release 12.2.7 and later, the check frequency is automatically set to 60 seconds. This check rate value cannot be changed.

- For prior versions of the ATG product family and EBS 12.2.6 and earlier, the UPDATE_CHECK_INTERVAL value is used to determine the refresh timing. The default value of UPDATE_CHECK_INTERVAL is 60 seconds.

Allowing a Host for Redirects

Now, `http://ebs.example.com:8000/OA_HTML/redirectTest.jsp` gives us an error stating "An invalid redirect has been blocked." This demonstrates the redirect blocking on.

Allow redirects to the specific custom page by using the following command:

```
$ cd $FND_TOP/secure
$ edit allowed_redirects.conf
```

Add in the following line in the manual configuration section:

```
host example.org
```

This will tell the system that it is allowed to redirect to this host.

Now, going to the page we've added (`http://ebs.example.com:8000/OA_HTML/redirectTest.jsp`) should redirect us to the custom page.

Headers during and after the redirect look like the following:

```
http://ebs.example.com:8000/OA_HTML/redirectTest.jsp

GET /OA_HTML/redirectTest.jsp HTTP/1.1
Host: ebs.example.com:8000
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=xxxx...; VIS1226_pses=xxxxx...
Connection: keep-alive

HTTP/1.1 302 Moved Temporarily
Date: Thu, 02 Mar 2017 18:10:04 GMT
Set-Cookie: JSESSIONID=xxxxxx...; path=/OA_HTML
Location: https://example.org/wiki/HTTP_302
Keep-Alive: timeout=15
Connection: Keep-Alive
Transfer-Encoding: chunked
...
-----------------------------------------------------------
https://example.org/wiki/HTTP_302

GET /wiki/HTTP_302 HTTP/1.1
Host: example.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: WMF-Last-Access=02-Mar-2017; WMF-Last-Access-Global=02-Mar-2017;
CP=H2; GeoIP=US:CA:Redwood_City:37.49:-122.24:v4;
enwikiGeoFeaturesUser2=xxxxxxxxxxxxxxxx; enwikimwuser-
sessionId=xxxxxxxxxxxxxxxx
Connection: keep-alive

HTTP/2.0 200 OK
Date: Thu, 02 Mar 2017 18:10:09 GMT
...
```

Finally, don't forget to turn the redirect filter back on by setting Allow Unrestricted Redirects to No, remove any redirects you added, and disable the JSP in the Allowed Resources UI.

When finished, remove the redirect host directive you added from `allowed_redirects.conf` and disable the JSP in the Allowed Resources UI.

You may also want to remove the test JSP and the associated Java and class files from the system, from both run and patch file systems:

```
$ rm $OA_HTML/redirectTest.jsp
$ rm $OA_HTML/WEB-INF/classes/_pages/__redirecttest.*
```

Troubleshooting Tips

Given the need to run and tweak access to redirects using this feature, you may find unexpected access errors - either access being permitted when you did not expect it would be, or (more commonly) access being denied when you expected it to be permitted.

For example, you may see an error with the text "An invalid redirect has been blocked."

This error is an expected behavior and is not a true error if the URL is accessed and it is not allowed (restricted). If the URL is accessed and it should be allowed (unrestricted), the error displayed is an error itself. Turn off the Allowed Redirects feature to determine where the redirect goes to understand what is being blocked and what may need to be added to the allowed redirects list.

5

Single Sign-On Integration

Overview of Single Sign-On Integration

This chapter is intended to provide guidance for those planning to deploy or integrate Oracle E-Business Suite Release 12.2 in an enterprise single sign-on environment. Aimed primarily at project managers, DBAs, and system administrators, it describes how to integrate Oracle E-Business Suite Release 12.2 with the appropriate supporting products to provide an enterprise-wide single sign-on solution.

> **Important:** Integration is a complex subject, with different components and sequences of steps being needed to accommodate different requirements. The integration options described require an understanding of the relevant products and deployment options.

In the context of this chapter, the term *integration* is used to refer to two closely related (but distinct) aspects of optionally deploying Oracle E-Business Suite in an enterprise-level single sign-on environment.

- Integration with a single sign-on product such as Oracle Access Manager (OAM)
- Integration with Oracle Directory Services (a Lightweight Directory Access Protocol, or LDAP, directory)

> **Note:** All occurrences of the acronym "OAM" in this chapter are references to the Oracle Access Manager product, and not to the completely unrelated Oracle Applications Manager product. All occurrences of the acronym "LDAP" in this chapter are references to the support LDAP directories. Currently, this is Oracle Directory Services (Oracle Internet Directory and Oracle Unified Directory). Any items that are specific to a directory type will reference the directory itself.

There is a mutual dependency: authenticating against LDAP requires use of a single

sign-on product (OAM), and deploying OAM requires the user population to be synchronized with Oracle Directory Services.

Oracle Access Manager

Oracle Access Manager 11g is the preferred Oracle single sign-on product for use with Oracle E-Business Suite Release 12.2. OAM also requires the use of *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.

As the single sign-solution for Oracle Fusion Middleware, Oracle Access Manager deals with user *authentication* (validating the user's identity). In contrast, user *authorization* (controlling what the user can access) is handled by Oracle E-Business Suite itself.

Oracle Directory Services

Oracle Directory Services refers to both Oracle Internet Directory (OID) and Oracle Unified Directory. Procedures documented for implementing Oracle Directory Services apply to both these directories.

Oracle Directory Services are needed to link the namespaces (user information repositories) employed by Oracle Access Manager and Oracle E-Business Suite respectively. 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 own FND_USER repository. The linking is done by associating externally-managed Oracle Access Manager users with internally-managed Oracle E-Business Suite users via Global Unique Identifiers (GUIDs). These GUIDs are generated by Oracle Directory Services, and the associated mapping functions are specific to it.

Oracle Directory Services are also required for another reason. While most usage of Oracle E-Business Suite is within an organization (such as a manufacturing company), certain application modules such as iRecruitment need to be available to outside users without accounts having to be created manually and responsibilities 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.

Combining Oracle Access Manager and Oracle Directory Services

Together, OAM and Oracle Directory Services enable an Oracle E-Business Suite Release 12.2 environment to provide the following enterprise single sign-on (SSO) features:

- Users can access multiple Oracle E-Business Suite Release 12.2 instances (or a mixture of Oracle E-Business Suite Release 12.2 and other single sign-on enabled applications) by logging in only once (single sign-on).

- A user who logs out of one SSO-enabled application is logged out of all others as well. This is sometimes called single sign-out, and improves security.
- Administrators and users can perform user management activities, such as account creation, deletion, at enterprise level.

Oracle Identity Manager

A further optional integration option is provided by *Oracle Identity Manager* (OIM), which provisions users from a central repository to other repositories such as Oracle Directory Services, third-party LDAPs such as Microsoft Active Directory, or non-LDAP repositories such as Oracle E-Business Suite's FND_USER. OIM can be used independently of OAM and Oracle Directory Services, or in conjunction with both.

Oracle Identity Manager includes *Connectors* for numerous *target systems* (IT resources) in an organization. For example, OIM provides Connectors for Oracle E-Business Suite that enable provisioning of users to the FND_USER table and the HRMS tables used by Trading Communities Architecture (TCA).

Introduction to Enterprise User Management

In large organizations, users often have a large number of userids for a variety of network-based resources such as corporate web sites and custom applications. As the number of available resources grow, users and security administrators are faced with the increasingly difficult challenge of managing a proliferation of userids and passwords across different systems.

Enterprise identity management solutions allow security administrators to define a user in a single location such as an LDAP (Lightweight Directory Access Protocol) directory and share that common user definition throughout multiple parts of their enterprise.

Oracle Identity Management may be integrated with Oracle E-Business Suite to support centralized user management through Oracle Directory Services, and to support single sign-on functionality by using Oracle Access Manager.

In its default configuration, Oracle E-Business Suite Release 12.2 allows registered users to log in using credentials stored directly in Oracle E-Business Suite. In this default configuration, Oracle E-Business Suite system administrators are responsible for maintaining the local repository of registered Oracle E-Business Suite users.

When optionally integrated with the Oracle Identity Management Suite (which includes OAM and Oracle Directory Services), Oracle E-Business Suite system administrators can reconfigure their environments to delegate both user administration and user authentication to Oracle Access Manager. This integration requires significant changes to how Oracle E-Business Suite Release 12.2 handles authentication. Instead of performing authentication natively, through the local Oracle E-Business Suite FND_USER table, Oracle E-Business Suite Release 12.2 now delegates this functionality to Oracle Access Manager, by using Oracle E-Business Suite AccessGate. In this

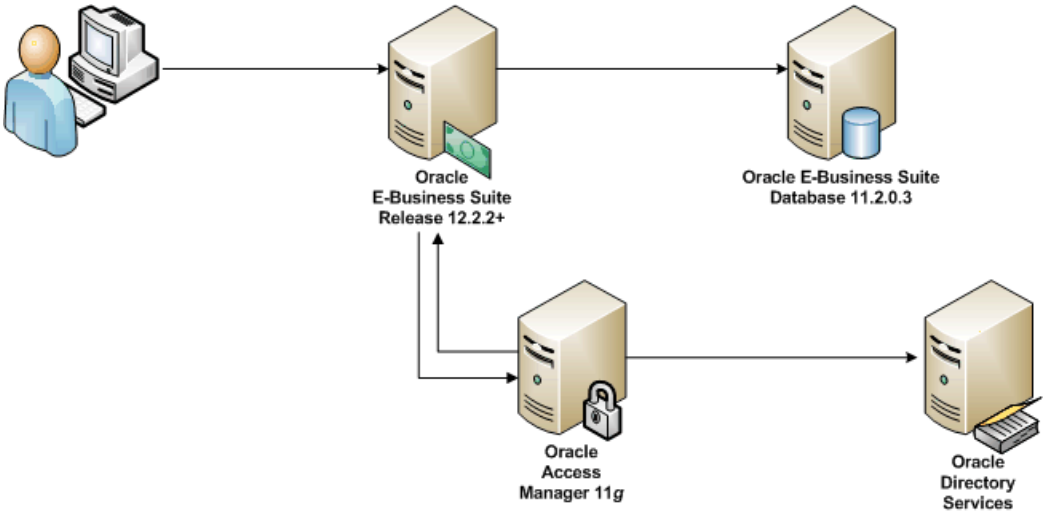
configuration, Oracle E-Business Suite Release 12.2 can direct unauthenticated users to Oracle Access Manager for identity verification and securely accept identities vouched for by the single sign-on mechanism.

Oracle Access Manager may, in turn, be integrated with existing third-party authentication systems such as Microsoft Windows (Kerberos), and Oracle Directory Services may be integrated with existing third-party LDAP directories such as Microsoft Active Directory.

> **Note:** Oracle Access Manager always performs authentication against information stored in Oracle Directory Services, even if a third-party authentication mechanism is in use.

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

High-Level Diagram of Typical Integration



> **Note:** Where a third-party authentication mechanism is in use, Oracle Access Manager and Oracle Directory Services are still required: they provide bridge functionality between Oracle E-Business Suite and the third-party single sign-on solution.

Integration Actions and Options

Integration of Oracle E-Business Suite with Oracle Access Manager is achieved by using the *OAM WebGate agent*, which is used in conjunction with Oracle E-Business Suite AccessGate.

Note: Each Oracle E-Business Suite instance requires its own deployment of the Oracle E-Business Suite AccessGate application.

Note: For a detailed description of the role of agents in Oracle Access Manager, refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

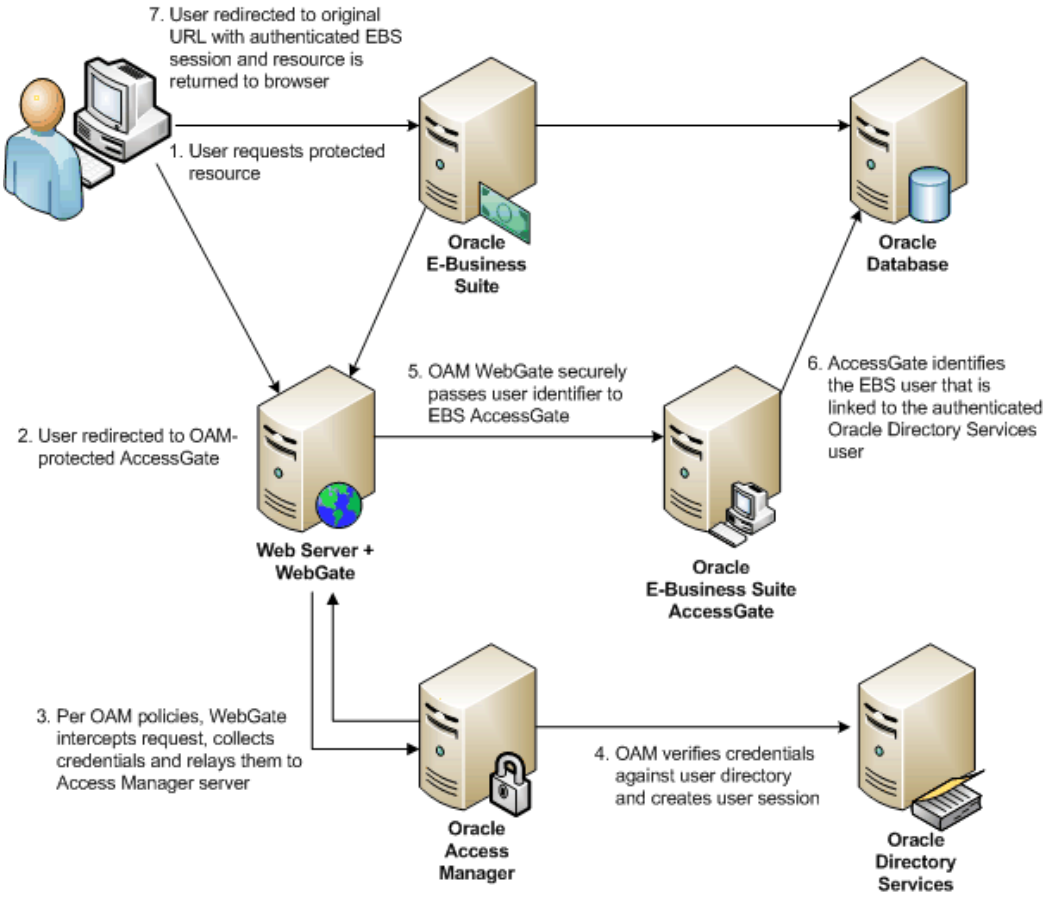
This section focuses on the details of integration using WebGate and Oracle E-Business Suite AccessGate.

When an unauthenticated user attempts to access a protected Oracle E-Business Suite resource, the user is directed to the Oracle E-Business Suite AccessGate application. This application is protected by the Oracle Access Manager server, so the authentication request is rerouted to a separate HTTP Server on which *Oracle Access Manager WebGate* is installed. This is a component of Oracle Access Manager that intercepts HTTP requests and redirects them to the Oracle Access Manager server to determine if and how the resources are allowed to be accessed, and to authenticate the current user if authentication is required. If Oracle Access Manager is already deployed in the environment, an existing WebGate can be configured for this purpose.

After a user is initially authenticated by Oracle Access Manager, the request for a resource and credentials returned by Oracle Access Manager server are picked up by Oracle E-Business Suite AccessGate. If the credentials are valid, Oracle Access Manager connects to the Oracle E-Business Suite database to link the Oracle Directory Services user to an Oracle E-Business Suite user. If Oracle E-Business Suite fails to identify a linked user for the Oracle Directory Services user, the user is redirected to the linking page so that he can map his unlinked Oracle Directory Services user account to his Oracle E-Business Suite user name. After this mapping is done, the originally requested resource is returned with a valid authenticated Oracle E-Business Suite user session. All subsequent requests for Oracle E-Business Suite resources are then returned directly to the user, for as long as the user session remains valid.

The sequence of actions is illustrated in the following diagram.

Integration Sequence Diagram



Oracle E-Business Suite AccessGate must be installed in the same internet domain (for example, example.com) as the Oracle E-Business Suite application tier servers. This is because several Oracle E-Business Suite domain cookies are shared between the application tier servers and the Oracle E-Business Suite AccessGate server.

Oracle E-Business Suite AccessGate Features

Forced Authentication

Similar to the session timeout behaviors, the Forced Authentication feature forces users to reauthenticate with Oracle Access Manager when ICX Session Timeout is reached. This happens regardless of whether OAM timeout has been reached.

The following are prerequisites for the Forced Authentication feature with Oracle E-Business Suite:

- Oracle E-Business Suite Release 12.2.3 through Release 12.2.11 with Patch 32651269.

- Integration with Oracle Access Manager 12c. For more information, refer to My Oracle Support Knowledge Document 2339348.1, *Integrating Oracle E-Business Suite Release 12.2 with Oracle Access Manager 12c using Oracle E-Business Suite Access Gate*.

- Deployment of Oracle E-Business Suite AccessGate 1.4 or later. For more information, refer to My Oracle Support Knowledge Document 2202932.1, *Using the Latest Oracle E-Business Suite AccessGate for Single Sign-On Integration with Oracle Access Manager*.

Forced Authentication is disabled by default (or "turned off"). It is controlled by profile option Applications SSO Force Authentication.

Profile Option Name	Code (Internal Name)
Applications SSO Force Authentication	APPS_SSO_FORCE_AUTH

Applications SSO Force Authentication can be set to either one of the following values:

- **Enabled**: The Forced Authentication feature is turned on when the profile APPS_SSO_FORCE_AUTH is set to Enabled. Enabled means on ICX session timeout, the user will be required to enter their user credentials, similar to Local login.

- **Disabled**: The Forced Authentication feature is turned off when the profile APPS_SSO_FORCE_AUTH is set to Disabled. Disabled means the user session will automatically be revalidated as long as the OAM session is not timed out or invalidated.

This profile option can be set at either site or user level.

Note that this feature requires /oamreauthenticate to be configured as a protected resource in OAM. Without configuring /oamreauthenticate as a protected resource, with APPS_SSO_FORCE_AUTH enabled on ICX Session Timeout when attempting to redirect to OAM login, the user will receive the following error: "The requested URL /oamreauthenticate was not found." See the Oracle Access Manager documentation for configuration details.

Limit SSO Sessions

Limit SSO Sessions is an Oracle E-Business Suite AccessGate feature available for Oracle E-Business Suite Release 12.2 which limits the user to only one active ICX session.

For example, if a user logs in from one browser or PC and then logs into another, since users are limited to only one active session all other sessions for that user will be timed out. If the user reauthenticates a session that was previously timed out, the newly reauthenticated session now becomes the single active session and all other sessions for that user will be timed out.

Limiting SSO Sessions requires the Forced Authentication feature (APPS_SSO_FORCE_AUTH) to be enabled.

Profile Option Name	Code (Internal Name)
Applications SSO Limit ICX Sessions	APPS_SSO_LIMIT_SESSIONS

If the user accesses a function and is redirected to the OAM Login page, they are able to reauthenticate and continue the session at which time any active ICX sessions will again be timed out.

Advanced Options and Configurations

Various options exist for extending the basic integration of Oracle E-Business Suite with Oracle Access Manager. These include using multiple WebGates for load balancing, enabling SSL communication between the nodes, and configuring one or more nodes in a DMZ or with a reverse proxy. This subsection will briefly mention any special Oracle E-Business Suite integration steps that may need to be taken for different Oracle Access Manager configurations.

Deploying Oracle E-Business Suite AccessGate in a TLS-Enabled Environment

In production environments, it is advisable to use TLS on both the Oracle E-Business Suite application tier and on the WebLogic Server instance where the Oracle E-Business Suite AccessGate is deployed. Also, the WebGate plug-in should be deployed on an HTTP server that is secured using TLS.

An important related point is that Oracle E-Business Suite application tiers and WebLogic Server instances must all be configured to use the same protocol (either HTTP or HTTPS). If the relevant nodes are configured to use TLS (HTTPS), the HTTP server on which WebGate is installed must also be configured to use TLS. If, however, the HTTP server running WebGate is configured to use TLS, it is not necessary to configure TLS on the Oracle E-Business Suite application tiers or WebLogic Server instances.

There are other considerations that apply to SSL environments. For further information, refer to the following resources:

- Steps to enable TLS communication for the Oracle Access Manager components: *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*
- Oracle WebLogic Server configuration steps: *Oracle Fusion Middleware Securing Oracle WebLogic Web Services for Oracle WebLogic Server*
- Oracle HTTP Server: *Oracle Fusion Middleware Administrator's Guide*

Deploying Oracle E-Business Suite AccessGate with an Oracle RAC Database

A database instance configured to use Oracle RAC load balancing requires creation of either a JDBC multidata source or Active GridLink for Oracle RAC. This can be done using the Oracle WebLogic Server Administration Console.

Once the multidata source has been created, an automated deployment script (`txkEBSAuth.xml`) can be run with the appropriate options.

This script performs two major functions, which can either be performed independently or together in a single execution. These functions are:

- Create a connection pool and data source for Oracle E-Business Suite AccessGate
- Deploy the Oracle E-Business Suite AccessGate war file with a customized application deployment plan

For more information, refer to *Oracle Fusion Middleware Administering JDBC Data Sources for Oracle WebLogic Server*.

Deploying Oracle E-Business Suite with Single Sign-On Integration in a DMZ

When configuring single sign-on using Oracle Access Manager and Oracle E-Business Suite AccessGate in a DMZ, specific firewall ports must be opened to allow additional connections from the end user to Oracle E-Business Suite AccessGate, and to allow communication between WebGate (located in the DMZ) and Oracle Access Server (located on the internal network). In addition, some of the values needed to configure Oracle E-Business Suite AccessGate will need to be modified to point back to a reverse proxy. There is no need to open the ports for LDAP or LDAPS connections from the DMZ to the internal network.

For more information, refer to My Oracle Support Knowledge Document 1375670.1, *Oracle E-Business Suite Release 12.2 Configuration in a DMZ*.

If you are using Oracle E-Business Suite Release 12.2.6 or later, you can choose to configure single sign-on and local authentication at site and at server level. For example, you may choose to register your Oracle E-Business Suite Release 12.2.6 or later instance with Oracle Access Manager for single sign-on at site level as the default for all internal users. For external users, you may not wish to register external entry points for single sign-on, but use local user authentication.

For more information, refer to My Oracle Support Knowledge Document 1576425.1, *Integrating Oracle E-Business Suite Release 12.2 with Oracle Access Manager 11gR2 (11.1.2) using Oracle E-Business Suite AccessGate*.

Centralized Logout

When logging out of an application protected by Oracle Access Manager, the host and domain cookies created by Oracle Access Manager are removed, which forces a user to re-authenticate the next time he accesses a protected resource. However, this process

does not clean up sessions, or remove cookies specific to partner applications such as Oracle E-Business Suite.

The process of logging out must invalidate all sessions for Oracle Access Manager, WebGate, and Oracle E-Business Suite. To ensure that these cookies are cleared when a single sign-on session is terminated, Oracle Access Manager and Oracle E-Business Suite AccessGate must be configured to initiate a "callback" to a script that will clean up these sessions. Without this, a user who terminates his single sign-on session may still be able to access Oracle E-Business Suite, or even create a new Oracle E-Business Suite session.

To help implement this functionality, a sample script called `samplecleanup.html` is provided. Using this script requires making some site-specific customizations to it, then configuring Oracle E-Business Suite AccessGate to load it. This file will subsequently be invoked whenever a user logs out of SSO, terminating any current sessions the user has for Oracle E-Business Suite instances protected by that WebGate.

The script works with Oracle E-Business Suite AccessGate to perform several actions:

1. Registers logout callbacks for the current Oracle E-Business Suite environment, and any others that are protected by this WebGate, which must be provided. This logout callback is a servlet within Oracle E-Business Suite AccessGate, which:
    1. Destroys the Oracle E-Business Suite session for the instance it is protecting
    2. Removes the ICX cookie
    3. Frees allocated E-Business resources
    4. Returns an image indicating success or failure
2. Processes the logout callbacks one by one, indicating success or failure.
3. Removes any cookies that are listed, such as WebGate 10g cookies, or session-related cookies for any custom applications that are deployed.
4. Redirects the user to a target URL (if one is provided) to control where a user is sent after the logout completes. The value of the target URL which will depend on where the user initiated the logout.

The `samplecleanup.html` script can be used regardless of where a user initiates the logout request. When logging out of Oracle E-Business Suite, Oracle E-Business Suite AccessGate will handle the logout process for the current instance, and then load this cleanup script on other WebGates (as configured in the script). As the scripts are loaded in parallel, the script also invokes a logout on the Oracle Access Manager server, which expires the Oracle Access Manager session and associated cookies. For external partner applications such as Oracle WebCenter, the logout link must be modified to invoke the cleanup script, which will redirect to the original logout URL or landing page upon completion.

The `samplecleanup.html` script has to be customized on a site-specific basis, as it must explicitly list the locations of every deployed Oracle E-Business Suite AccessGate application that is protected by the WebGate in question. The customized script must then be deployed to the server where WebGate is installed, so the Oracle Access Manager Server can load it.

Enterprise User Management

Oracle Directory Services is the integration point that allows Oracle E-Business Suite to participate in enterprise-level user management. 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 through 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.

Another requirement in such an 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 support for automatic propagation of user information across an enterprise:

- A *synchronization* process between Oracle Directory Services and a third-party LDAP server
- A *provisioning* process between Oracle Directory Services and Oracle E-Business Suite

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 document provides mechanisms to link the existing data together using the GUID. In addition, bulk migration tools are provided to move a large number of users between Oracle Directory Services and Oracle E-Business Suite during the transition to a single sign-on environment.

Additional Single Sign-On Features, Limitations, and Known Issues

Advanced features include automatically keeping a set of user profile information synchronized across an enterprise for an entity, and the ability to link an account in Oracle Directory Services to multiple application accounts in Oracle E-Business Suite.

In this release, provisioning from Oracle E-Business Suite to Oracle Directory Services is synchronous: that is, all user management operations carried out in Oracle E-Business Suite are also carried out in Oracle Directory Services. However, provisioning from Oracle Directory Services to Oracle E-Business Suite is done asynchronously.

The solution described here does not address the issue of *authorization*. After a user has been authenticated, Oracle E-Business Suite retrieves from the relevant FND tables 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.

Key Identity Management Configuration Options

Configuration Option	Possible Settings	Configured Using
Initial Source of User Information	• Oracle E-Business Suite. • Oracle Directory Services. • Third-Party LDAP Directory. • A combination of the above.	Execution of manual initial provisioning steps (described later).
Source of Truth for Updates to User Information	• Oracle E-Business Suite. • Oracle Directory Services. • Third-Party LDAP Directory. • A combination of the above.	Provisioning profile selected for Oracle Directory Integration Platform (described later).

Configuration Option	Possible Settings	Configured Using
New Userids Created in Oracle Directory Services	• Are automatically created in Oracle E-Business Suite with subscriptions for user attribute updates. • Have manually-created equivalent userids in Oracle E-Business Suite, and are manually linked by the end-user at the time of first logon. • Have manually-created equivalent userids in Oracle E-Business Suite, and are automatically linked at the time of first logon. • Are automatically created in a third-party LDAP directory, combined with either of the two above options.	Related Oracle E-Business Suite Profile Options: • APPS_SSO_OID_IDENTITY • APPS_SSO_AUTO_LINK_USER • APPS_SSO_LINK_SAME_NAMES

Configuration Option	Possible Settings	Configured Using
New Userids Created in Oracle E-Business Suite	• Are automatically created in Oracle Directory Services with subscriptions for user attribute updates. • Have manually-created equivalent userids in Oracle Directory Services, and are manually linked by the end-user at the time of first logon. • Have manually-created equivalent userids in Oracle Directory Services, and are automatically linked at the time of first logon.	Related Oracle E-Business Suite Profile Options: • APPS_SSO_LDAP_SYNC • APPS_SSO_AUTO_LINK _USER
Specific Oracle E-Business Suite Userids	• Log in to Oracle E-Business Suite using Oracle Access Manager. • Log in to Oracle E-Business Suite directly. • Both of the above.	APPS_SSO_LOCAL_LOGIN profile option
All Oracle Directory Services Userids	• Are linked to a single Oracle E-Business Suite userid. • Are linked to multiple Oracle E-Business Suite accounts.	APPS_SSO_ALLOW_MULTI PLE_ ACCOUNTS profile option

The above list of identity management configuration options is not exhaustive.

Deployment Scenario 0: E-Business Suite + SSO and Oracle Directory Services

This section explains the technical details and deployment steps using a simplified deployment scenario, where an existing Oracle E-Business Suite instance is integrated with a fresh Oracle Access Manager/Oracle Directory Services infrastructure. Although many real world deployments are likely to be more complex, this scenario serves to illustrate the core concepts and procedures of the integration effort. In later sections, we build on this basic scenario to describe more sophisticated situations such as the existence of a third-party single sign-on solution, or the presence of multiple user repositories. The goal is not to describe every conceivable deployment variation, but rather to provide a number of representative cases from which implementers can intelligently derive the exact steps needed for their particular requirements.

Starting Point

This scenario presumes that:

- Oracle E-Business Suite Release 12.2 has been installed and has an existing user population.
- Oracle Access Manager, Oracle E-Business Suite AccessGate, and Oracle Directory Services have all been installed (on a separate machine) in accordance with the appropriate instructions.
- 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, Oracle E-Business Suite AccessGate, and Oracle Directory Services.

Solution Outline

The results of implementing this solution will be that:

- Oracle E-Business Suite will delegate user sign-on and authentication to Oracle Access Manager.
- Oracle Access Manager will authenticate user credentials against user entries in Oracle Directory Services.
- Oracle Directory Services will contain the account ID and password for every user that is configured for single sign-on.

Warning: For security reasons, local users and standard

administrative accounts such as SYSADMIN should never be configured for single sign-on.

Deployment Scenario Flow

User Management Options

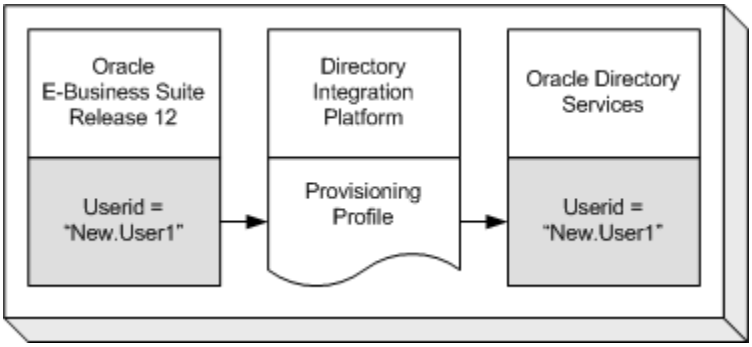
Oracle E-Business Suite Release 12.2 maintains a local cache of user information in its existing user directory (FND_USER). The Oracle E-Business Suite User Bulk Migration Tool can be used to migrate existing Oracle E-Business Suite application accounts to single sign-on accounts in Oracle Directory Services. After the migration, a system administrator has a number of user management options about the locations where the user information is created, and where it is provisioned (sent).

Option 1: Provision Oracle E-Business Suite Users to Oracle Directory Services

All user information is created in Oracle E-Business Suite, then provisioned into Oracle Directory Services: Oracle E-Business Suite is configured as a *provisioning integrated application* with Oracle Directory Services. System administrators configure the provisioning integration by using Directory Integration Platform (DIP) *provisioning profiles*. A DIP server synchronizes policy changes in the directory with connected databases, using a separate DIP provisioning profile for each database.

The creation of a new application account in Oracle E-Business Suite 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 1 Flow



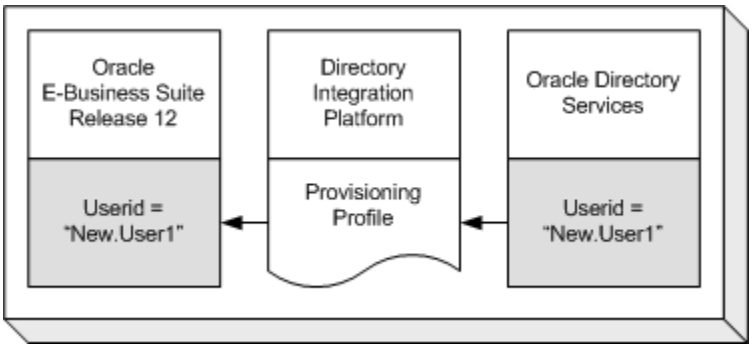
Option 2: Provision Oracle Directory Services Users to Oracle E-Business Suite

All user information is created in Oracle Directory Services, then provisioned into Oracle E-Business Suite. Oracle E-Business Suite is configured as a provisioning integrated application with Oracle Directory Services.

System administrators configure the provisioning integration using provisioning profiles: 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. 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.

With provisiontype=3 (OID to App), the OID Enterprise Manager console shows both 'Applications to OID' and 'OID to Applications' enabled. This is expected due to the need to make use of the SUBSCRIPTION_ADD event for the 'Applications to OID' provisioning profile. The user is added to the subscription list once the user is successfully created on the Applications side.

Option 2 Flow



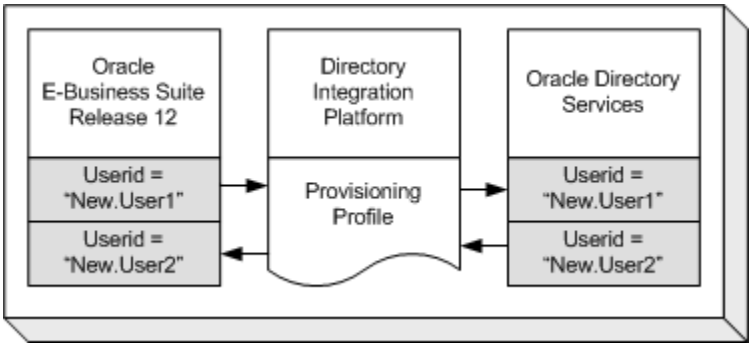
Option 3: Bidirectional Provisioning Between E-Business Suite and Oracle Directory Services

All user information is created in either Oracle Directory Services or Oracle E-Business Suite, then provisioned into the other system. Oracle E-Business Suite is configured as a provisioning integrated application with Oracle Directory Services. System administrators configure the provisioning integration using provisioning profiles.

The creation of a new application account in Oracle E-Business Suite will automatically trigger the creation of a new single sign-on account in Oracle Directory Services. 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.

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

Option 3 Flow



Synchronizing User Attributes

For all three options above, a predefined set of user attributes is synchronized between Oracle E-Business Suite and Oracle Directory Services. Currently-supported attributes are listed later in the Supported Attributes, page 5-93 section.

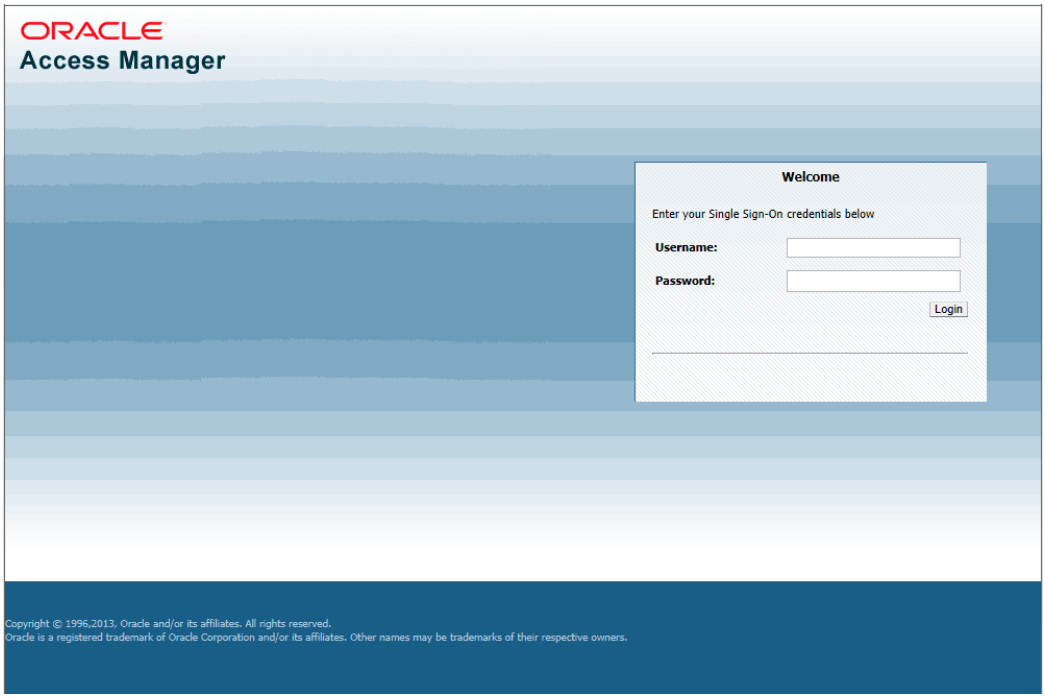
End-User Experience

This section describes the user's perception of the single sign-on environment.

Single Sign-On User Experience

On attempting to access an Oracle E-Business Suite environment, a user who has not yet been authenticated with Oracle Access Manager is directed to a single sign-on login page:

Oracle Access Manager Single Sign-On Login Page



After authentication using Oracle Access Manager (or if authentication has previously been carried out), the user is redirected to the requested page or the user's home page in Oracle E-Business Suite Release 12.2.

Sign-Out User Experience

When a user logs out of an Oracle E-Business Suite instance, he is also logged out of Oracle Access Manager, as well as any other applications (partner applications) that have been integrated with Oracle Access Manager and have been accessed through Oracle Access Manager.

Single Sign-On Authentication Flow

The user attempts to access the Oracle E-Business Suite Release 12.2 instance, and Oracle E-Business Suite looks for a session cookie. If the cookie is found and validated, the user is directed to the requested application page, and the rest of the steps shown here are skipped.

If the session cookie is not found, Oracle E-Business Suite redirects the user to an Oracle E-Business Suite AccessGate URL in Oracle Access Manager. This URL is intercepted by OAM WebGate, which obtains policy information from OAM and then checks for a valid OAM session cookie in the user's browser. If one does not exist, it redirects the user to the credential collection page, which is an unprotected page in AccessGate. The credentials are submitted to OAM, which looks for an Oracle Single Sign-On security cookie in the user's browser. If the Oracle Single Sign-On security cookie is not found,

the user must log into a valid account by using Oracle Access Manager before authentication can proceed further.

Next, Oracle Access Manager contacts Oracle Directory Services and authenticates the user's credentials against the list of registered users in Oracle Directory Services. After successful authentication, Oracle Access Manager sets an OAM session cookie in the user's browser, and retrieves user attributes for the single sign-on account from Oracle Directory Services.

Once the credentials are verified, OAM returns the user to the URL in Oracle E-Business Suite AccessGate. It passes a request that includes HTTP response headers containing a user identifier and the GUID. Oracle E-Business Suite verifies the URL token, locates the application user and creates an application session and corresponding cookie, based upon the user's assigned application responsibilities and roles. This process entrusts the process of user authentication to Oracle Access Manager, and user authorization to Oracle E-Business Suite. Oracle E-Business Suite then redirects the user to the requested application page, or the user's home page.

Session Timeout Behavior

When both the application session and the single sign-on session timeout, the user will be directed to the single sign-on login page to re-authenticate. After a successful re-authentication, the user will be redirected back to Oracle E-Business Suite. The application page the user sees depends on the application technology stack in use; see table below.

Currently, when the application session has expired, but not the single sign-on session, the user will be directed to Oracle E-Business Suite AccessGate, and then back to Oracle E-Business Suite Release 12.2, without being prompted to re-authenticate. Depending on the technology stack in use at the time when the session timeout occurred, the user will then see one of the following pages listed in the table below.

Session Timeout Behaviors

Technology Stack	Session Timeout Behavior
Oracle Application Framework	Application home page
CRM	If the current request on detection of application session expiration was a 'GET', the user sees the requested page. If the current request was a 'POST', the user sees the posting page without the post having been performed.

Technology Stack	Session Timeout Behavior
Forms	A series of pop-up windows will appear, leading the user to the Oracle Access Manager login page for re-authentication.

When an application session is terminated because the maximum valid period has been reached, or because of a period of user inactivity, Oracle E-Business Suite redirects the user to Oracle Access Manager for re-authentication. Oracle Access Manager checks the single sign-on cookie; if it is still valid, the user is redirected back to Oracle E-Business Suite Release 12.2. If the single sign-on cookie has expired as well, Oracle Access Manager requires the user to authenticate again before redirecting him back to Oracle E-Business Suite Release 12.2.

The application session timeout value takes precedence over the Oracle Access Manager timeout settings. For example, until an application session times out (or the user explicitly logs out), a user may continue to access the partner application even if his Oracle Access Manager security cookie has expired. We therefore recommend setting Oracle E-Business Suite's application session timeout value to be equal to, or less than, that of the Oracle Access Manager server.

User Management Options

This section describes the various options for management of users in a single sign-on environment.

Local Access to Oracle E-Business Suite

Selected users can be permitted to log in to the application directly, that is, without going through the single sign-on process. This allows users such as the system administrator to troubleshoot a configuration when Oracle Access Manager is not functioning correctly, or is unavailable. Such local users can now log into the application directly by using the applications login page, AppsLocalLogin.jsp. The supplied `SYSADMIN` account is configured to have local access. In addition, the `SYSADMIN` account can control which additional users (if any) are permitted to have local access to the Oracle E-Business Suite; this is accomplished through the Applications SSO Login Types (`APPS_SSO_LOCAL_LOGIN`) profile option.

> **Important:** Generic accounts, especially those with administrative rights (such as SYSADMIN), should always be local only.

Identifying a User Across the Enterprise

After Oracle Access Manager integration is complete, user information exists in two places: Oracle Directory Services and Oracle E-Business Suite Release 12.2.

This shared information has the following characteristics:

- A GUID uniquely identifies a user across multiple systems.
- Both Oracle Directory Services and Oracle E-Business Suite store GUID information for each single sign-on user.
- During the authentication handshake between Oracle Directory Services and Oracle E-Business Suite, Oracle Access Manager passes the authenticated user information in the form of GUID to Oracle E-Business Suite AccessGate, which then uses the GUID to locate the corresponding application account.
- Once a GUID is generated and stored in both a single sign-on account in Oracle Directory Services and an application account in Oracle E-Business Suite, the two accounts are said to be linked.
- A number of processes are used to establish this link. The most commonly used ones are explained below, and the rest in the more advanced deployment scenarios later in this section.

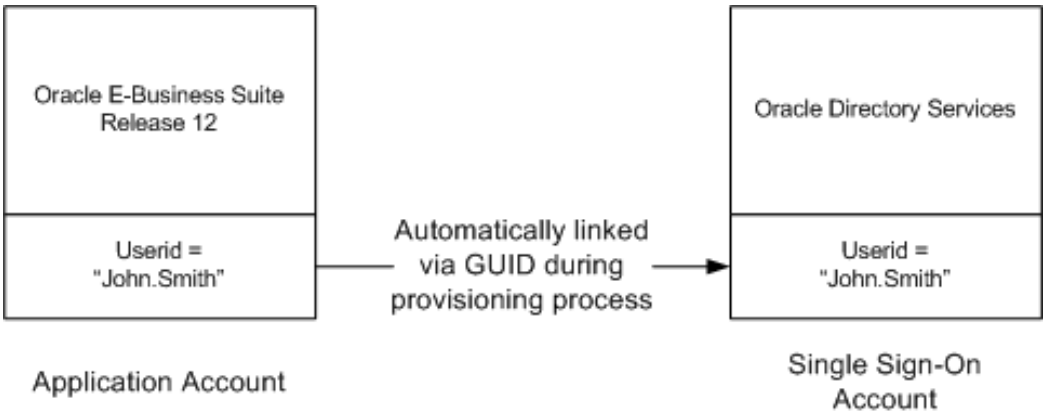
Bulk Migration of Users

Tools are provided to migrate existing users in bulk between Oracle Directory Services and Oracle E-Business Suite. Both Oracle Directory Services and Oracle E-Business Suite provide command-line utilities to export and import users using flat text files in LDIF format.

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

New users created on either system can be provisioned into the other through the provisioning process. The provisioning system consists of components of both Oracle Directory Services and Oracle E-Business Suite that queue user events on each system, plus an Oracle Directory Services process that periodically pushes or pulls these events to or from Oracle E-Business Suite. The provisioning process establishes the GUID link for provisioned accounts. During this process, single sign-on accounts are automatically linked to Oracle E-Business Suite application accounts.

Diagram of User Provisioning Between Oracle E-Business Suite and Oracle Directory Services



Provisioning has the following characteristics:

- Once linked, user changes from either system can be provisioned into the other.
- The provisioning process between Oracle Directory Services and each Oracle E-Business Suite instance is determined by a provisioning profile.
- The provisioning profile controls which user events are provisioned, the direction of provisioning, and the user attributes included in each event.
- Oracle E-Business Suite is said to be a provisioning integrated application with Oracle Directory Services when a provisioning profile is created for it.

Refer to the Supported Attributes, page 5-93 section for information on which attributes can be provisioned between the systems, and Configuring Directory Integration Platform Provisioning Templates, page 5-66 for more details on the provisioning process.

Strategies for User Management

At the start of the deployment, Oracle E-Business Suite Release 12 is the sole repository of user information. Users who will need to access Oracle E-Business Suite using Oracle Access Manager must already exist or be created in Oracle Directory Services.

For pending users that are enabled in Oracle E-Business Suite after user creation, the IDENTITY_MODIFY event from Oracle E-Business Suite to Oracle Directory Services must be enabled.

> **Note:** Refer to Configuring Directory Integration Platform Provisioning Templates, page 5-66 for more details.

Populating Oracle Directory Services with Existing Oracle E-Business Suite Users

Existing Oracle E-Business Suite users can be migrated into Oracle Directory Services by means of the bulk migration tool (see Migrating Data Between Oracle E-Business Suite and Oracle Directory Services, page 5-78 for details).

Creating New Users

After the initial migration, you may choose to allow new users to be created either from Oracle Directory Services or from Oracle E-Business Suite, and then provision them into the other system. This is achieved by enabling either the SUBSCRIPTION_ADD event from Oracle Directory Services to Oracle E-Business Suite, or the IDENTITY_ADD event from Oracle E-Business Suite to Oracle Directory Services. Refer to Configuring Directory Integration Platform Provisioning Templates, page 5-66 for more details.

Bidirectional Provisioning

Alternatively, you may choose to create new users from either Oracle Directory Services or Oracle E-Business Suite, and then provision them into the other system. This is achieved by enabling both the SUBSCRIPTION_ADD event from Oracle Directory Services to Oracle E-Business Suite, and the IDENTITY_ADD event from Oracle E-Business Suite to Oracle Directory Services. Refer to Configuring Directory Integration Platform Provisioning Templates, page 5-66 for more details.

Bidirectional provisioning requires careful planning, and the following restrictions must be considered:

- The provisioning process from Oracle Directory Services to Oracle E-Business Suite is *asynchronous*. In contrast, the provisioning process from Oracle E-Business Suite to Oracle Directory Services is *synchronous*.

- Whether new users are created in either Oracle Directory Services or Oracle E-Business Suite, they must be granted the appropriate roles or responsibilities using Oracle E-Business Suite User Management in order to access application functionality.

- The provisioning events will fail if, for example, a user with the same user name has been created concurrently on the other system, or some aspect of the user's profile does not meet the policy set on the other system. As there is no mechanism to roll back the original change on the system that triggered the event, the failure can put the entire system into an unstable state. It is therefore essential to coordinate the account policy on all the systems involved, and place appropriate safeguards on the user creation process. For example, user names created directly on one system need to be chosen in the context of names used across the single sign-on environment.

Updating User Information

User information stored in Oracle Directory Services single sign-on accounts is generally managed independently of user information stored in Oracle E-Business Suite

Release 12.2 application accounts.

System administrators must decide:

- Which user attributes are to be provisioned between an Oracle E-Business Suite Release 12.2 instance and Oracle Directory Services.

- Which system is to be the primary "source of truth" for a given attribute. This determines the provisioning direction for that attribute.

System administrators then enable the IDENTITY_MODIFY events in the appropriate direction with the appropriate attribute list. Refer to Configuring Directory Integration Platform Provisioning Templates, page 5-66 for more details.

Note the following current restrictions:

- Updates to email ID in Oracle Directory Services are not correctly reflected in Oracle E-Business Suite (HZ_CONTACT_POINTS in TCA) unless the PERSON_PARTY_ID foreign key in the FND_USER table has been defined. Furthermore, if PERSON_PARTY_ID is changed, because a user is linked to another person in TCA, information stored in Oracle Directory Services can overwrite this other person's information during provisioning.

- Provisioning from Trading Community Architecture (TCA) to Oracle Directory Services is not supported.

- Provisioning of data from Oracle Human Resources to Oracle Directory Services is supported through the Oracle Human Resources Agent, which is released as part of the Oracle Directory Services suite of utilities. Note that the Oracle Human Resources Agent supplied with Oracle Directory Services is unidirectional. That is, it ensures that Oracle Directory Services is synchronized with HR, so that changes to user data in HR cause the corresponding data to be updated in Oracle Directory Services. However, if changes are made to user data in Oracle Directory Services, the HR connector does not synchronize these changes back to HR. A bidirectional connector is planned for a future build.

Terminating and End-Dating Users

Dates are not synchronized between Oracle Directory Services and Oracle E-Business Suite. However, the provisioning process may be set up so that when a single sign-on account in Oracle Directory Services is deleted, the associated Oracle E-Business Suite application accounts is end-dated. This is accomplished in the provisioning profile, by enabling the IDENTITY_DELETE event from Oracle Directory Services to Oracle E-Business Suite.

> **Note:** Refer to Configuring Directory Integration Platform Provisioning Templates, page 5-66 for details.

Subject to organizational security and audit policies, it may be preferable to disable single sign-on accounts in Oracle Directory Services rather than delete them, since this

allows an applications account to be re-enabled at a later date as required. This can be particularly useful in the case of contractors who may leave and rejoin.

> **Additional Information:** See Enabling and Disabling Users, page 5-91 for more information on enabling/disabling users.

Password Management

One of the major objectives of single sign-on integration is centralized user password management using Oracle Directory Services, which provides the following features:

- Accessing Oracle E-Business Suite using Oracle Access Manager does not require passwords in the Oracle E-Business Suite; the password stored in Oracle Directory Services is sufficient for authentication.
- The password for an application account in Oracle E-Business Suite Release 12.2 is replaced with the reserved keyword 'EXTERNAL', if (as will usually be the case) the only permitted method to access that application account is through Oracle Access Manager
- Password management for such users is carried out entirely in Oracle Directory Services.

End-User Password Changes

The majority of end users will be able to change their single sign-on passwords using the standard methods provided by Oracle Directory Services. For example, users may employ Oracle Identity Manager.

System Administrator Password Changes and Resets

To reset single sign-on passwords, an administrator using Oracle Directory Services should follow the methods detailed in the "Managing Accounts and Passwords" chapter of the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* and "Managing User Accounts" section of *Oracle Fusion Middleware Administering Oracle Unified Directory*.

Password Policies

Oracle Directory Services is designated as the primary user directory for passwords. The user's password creation, modification and Oracle Access Manager login activities are subject to the Oracle Directory Services rules that govern how passwords are created and used. For example, Oracle Directory Services system administrators may establish policies for password expiration, minimum length, and alphanumeric mixes. Refer to either the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* or *Oracle Fusion Middleware Administering Oracle Unified Directory*, depending

which is used, for an explanation of supported password policies.

If the provisioning profile specifies that passwords in application accounts are to be provisioned from Oracle E-Business Suite Release 12.2 to Oracle Directory Services, Oracle E-Business Suite Release 12.2 password policies must be at least as restrictive as the ones in Oracle Directory Services. This ensures that passwords can be successfully propagated from Oracle E-Business Suite Release 12.2 to the single sign-on accounts in Oracle Directory Services.

> **Note:** Passwords stored in Oracle Directory Services are case sensitive. Mixed case passwords in Oracle E-Business Suite are migrated with the case preserved.

Password Management and Applications SSO Login Types

For users who have been granted local access to Oracle E-Business Suite by using the Applications SSO Login Types (APPS_SSO_LOCAL_LOGIN) profile, Oracle E-Business Suite retains the relevant applications account password. This is true even if Oracle Directory Services or the third-party LDAP directory has been designated as the primary user directory for passwords. All existing password-related features in the Oracle E-Business Suite remain the same for local accounts. For example, the user must use the Self-Service change password screen (Preferences page) to maintain passwords.

For users who have both single sign-on and local access to Oracle E-Business Suite, local password change in Oracle E-Business Suite can be synchronized to Oracle Directory Services, if the provisioning profiles are set up accordingly. The reverse direction is not possible, because Oracle Directory Services only stores the hash of the passwords, not encrypted passwords as Oracle E-Business Suite does.

Because of the potential difficulty of educating users about the special password management considerations that apply to application accounts configured with the Applications SSO Login Types (APPS_SSO_LOCAL_LOGIN) profile, this profile option should, as noted earlier, only be employed for a limited number of system administration or other advanced accounts. The system administrator is required to set the local password using the AFPASSWD utility or FNDCPASS utility, in case user passwords stored only in LDAP (APPS password is set to EXTERNAL) also need to be stored locally in Oracle E-Business Suite.

For more information about the AFPASSWD and FNDCPASS utilities, refer to the *Oracle E-Business Suite Maintenance Guide*.

Critical Implementation Decisions

1. Oracle Directory Services has a powerful and flexible set of configuration options. Most Oracle E-Business Suite system and security administrators will be able to use the default Oracle Directory Services configuration. Security administrators with advanced security requirements may choose to use alternative Oracle Directory

Services configurations.

Items of particular importance to Oracle E-Business Suite integration include:

- Identity management realm
- DIT structure
- What attribute is chosen as the nickname attribute
- Whether new users are to be created:
  - Only from Oracle Directory Services
  - Only from Oracle E-Business Suite Release 12.2
  - From both Oracle E-Business Suite and Oracle Directory Services

2. Whether updates to user information are to be provisioned. If so, what user attributes are to be provisioned, and the direction of provisioning.
3. Which users should only use local access to Oracle E-Business Suite Release 12.2, which users only need access through Oracle Access Manager, and which users need both types of access.
4. Oracle Access Manager settings:
   - Session timeout values for both Oracle E-Business Suite and Oracle Access Manager.
   - Password policy for both Oracle E-Business Suite and Oracle Identity Management.

Implementation Instructions

1. Identify the user population that only need local login access to Oracle E-Business Suite, and set the Applications SSO Login Types (APPS_SSO_LOCAL_LOGIN) profile accordingly for those users (see: Single Sign-On Profile Options, page 5-52).
2. Configure session time out values in both Oracle E-Business Suite Release 12.2 and Oracle Single Sign-On.
3. Configure password policies, as appropriate, in Oracle Directory Services and Oracle E-Business Suite.
4. Migrate existing Oracle E-Business Suite accounts to Oracle Directory Services using the Oracle E-Business Suite User Bulk Migration Tool (see: Migrating Data

Between Oracle E-Business Suite and Oracle Directory Services, page 5-78).

5. Set Oracle E-Business Suite profile options (see: Single Sign-On Profile Options, page 5-52).

Recommended Profile Option Values

Profile Option Name (Internal Name)	Recommended Value
Applications Authentication Agent (APPS_AUTH_AGENT)	Set to the location of the Oracle E-Business Suite AccessGate login page.
Applications SSO Type (APPS_SSO)	Set to 'SSWA w/SSO' to switch to Single Sign-On mode.
Self-Service Personal Home Page mode (APPLICATIONS_HOME_PAGE)	Set to the desired choice of home page.
Applications SSO Login Types (APPS_SSO_LOCAL_LOGIN)	At the site level, set the value to be the usage mode the majority of users will be in. Override at the user level for users who have special needs.
Applications Local Login URL (APPS_LOCAL_LOGIN_URL)	If using a customized local login page, set the value to be the name of the page, otherwise leave unchanged.
Applications SSO Auto Link User (APPS_SSO_AUTO_LINK_USER)	Set as needed. See: Single Sign-On Profile Options, page 5-52.
Applications SSO Allow Multiple Accounts (APPS_SSO_ALLOW_MULTIPLE_ACCOUNTS)	Leave unchanged.
Applications SSO LDAP Synchronization (APPS_SSO_LDAP_SYNC)	Leave unchanged at the site level, override at user level for users with special needs.
Applications Local Change Password URL (APPS_LOCAL_CHANGE_PWD_URL)	Leave unchanged unless using a customized self-service change password page to change passwords in Oracle E-Business Suite Release 12.
Applications SSO Change Password URL (APPS_SSO_CHANGE_PWD_URL)	Set to the absolute URL for self-service password change page in Oracle Directory Services.

Profile Option Name (Internal Name)	Recommended Value
Applications SSO Enable OID Identity Add Event (APPS_SSO_OID_IDENTITY)	Set as needed. See: Single Sign-On Profile Options, page 5-52.
Applications SSO Link Same Names (APPS_SSO_LINK_SAME_NAMES)	Indicates whether the Oracle E-Business Suite Release 12.2 instance should link a newly-created Oracle E-Business Suite user to an existing Oracle Directory Services account with the same name.

Deployment Scenario 1: Multiple Oracle E-Business Suite Instances + Central SSO and Oracle Directory Services Instance

This section and the following three present more sophisticated deployment scenarios. The solutions given should be interpreted as guidelines or building blocks rather than definitive instructions, as all real world deployments will be unique. In the cases presented, the solutions are built upon the basic scenario discussed above, and only highlight those actions that are different from or additional to, the basic one.

Starting Point

- Multiple new Oracle E-Business Suite environments (Release 12.0.0 and later) have been installed using Rapid Install. Other than the default seeded administrative accounts, no user accounts have been registered yet.
- No single sign-on infrastructure in place.

Architectural Requirements

This scenario applies when a customer wants to integrate multiple new Oracle E-Business Suite Release 12.2 environments with a single Oracle Access Manager instance.

Solution Outline

- Oracle Access Manager, Oracle E-Business Suite AccessGate, and Oracle Directory Services are needed for the integration required. All the installations of Oracle E-Business Suite Release 12.2 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 (except those such as `SYSADMIN` that are configured for local access only).

- Either Oracle Directory Services or one Oracle E-Business Suite Release 12.2 instance can be designated as the source of user enrollment. If Oracle Directory Services is the source, details of user accounts can be propagated to each Oracle E-Business Suite instance by using 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.

- *Optional*: User profile information in an Oracle E-Business Suite Release 12.2 instance can be kept synchronized with the information in Oracle Directory Services.

Solution Details

User Management Options

In this solution, the system administrator must decide which component will be the point of user enrollment and the source of truth for user information. Either Oracle Directory Services or an Oracle E-Business Suite instance can be chosen for this role.

1. Oracle Directory Services is the point of user enrollment and source of truth.

   - After a user is created in Oracle Directory Services, the user identity can be propagated to each Oracle E-Business Suite instance using the provisioning process. To accomplish this, the provisioning profile for each Oracle E-Business Suite Release 12.2 instance needs to enable the SUBSCRIPTION_ADD event from Oracle Directory Services to Oracle E-Business Suite Release 12.2.

   - *Optional*: The provisioning profile can also be configured such that user profile information change in Oracle Directory Services can be propagated to each Oracle E-Business Suite Release 12.2 instance. To accomplish this, the provisioning profile for each Oracle E-Business Suite Release 12.2 instance needs to enable the IDENTITY_MODIFY event from Oracle Directory Services to Oracle E-Business Suite Release 12.2.

2. An Oracle E-Business Suite Release 12.2 instance is designated as the point of user enrollment and source of truth (the primary instance).

   - After a user is created from the primary Oracle E-Business Suite Release 12.2 instance, the provisioning process can be used to propagate the user identity first to Oracle Directory Services, then to other Oracle E-Business Suite Release 12 instances. To accomplish this, the provisioning profile for the primary Oracle E-Business Suite Release 12.2 instance needs to enable the IDENTITY_ADD

event from Oracle E-Business Suite Release 12.2 to Oracle Directory Services. The provisioning profile for the rest of the Oracle E-Business Suite Release 12.2 instances needs to enable the SUBSCRIPTION_ADD event from Oracle Directory Services to Oracle E-Business Suite Release 12.2.

Deployment Scenario 2: New Oracle E-Business Suite Installation + Existing Third-Party Identity Management Solution

This section presents a slightly more sophisticated deployment scenario.

Starting Point

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

Architectural Requirements

Need to integrate new installation of Oracle E-Business Suite Release 12.2 with existing third-party single authentication mechanisms and third-party LDAP directory infrastructure.

Solution Outline

- Oracle Access Manager, Oracle E-Business Suite AccessGate, and Oracle Directory Services are used for integration with third-party authentication mechanisms or third-party LDAP directories.

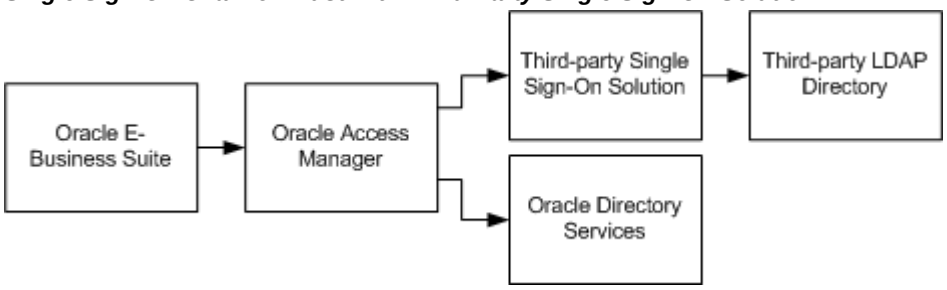
  Note: Integrating Oracle E-Business Suite directly with third-party authentication mechanisms or third-party LDAP directories is not supported.

- Oracle E-Business Suite and Oracle Access Manager need to be set up to enable Oracle E-Business Suite delegation of authentication to Oracle Access Manager, which in turn delegates the functionality to the third-party single sign-on authentication mechanism.

  The following is the Single Sign-On Chain of Trust with Third-Party Single Sign-On

Solution:

Single Sign-On Chain of Trust with Third-Party Single Sign-On Solution



- Oracle Directory Services needs to be set up to synchronize a minimal set of user attributes when integrating with a third-party LDAP directory. Refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* or *Oracle Fusion Middleware Administering Oracle Unified Directory* for more information about performing this integration.

- User information from the third-party LDAP directory for all users who will access Oracle E-Business Suite using single sign-on. Oracle Directory Services also needs to be set up to provision users in Oracle Directory Services to Oracle E-Business Suite.

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

- *Optional*: A set of user profile information in Oracle E-Business Suite can be kept synchronized with the information in the third-party LDAP directory.

End-User Experience

Single Sign-On User Experience

- **Sign on process**: the sign on user experience is the same as that in the base scenario, except that the login page is served by the third-party authentication mechanism.

- **Sign out process**: when a user logs out from Oracle E-Business Suite Release 12.2, Oracle Access Manager logs the user out of all registered Oracle partner applications. The user is also logged out of the third-party single sign-on solution, if the administrator has set this up in the `samplecleanup` script.

- **Session timeout**: the session timeout user experience is the same as that in the base scenario, except that the user will be asked to re-authenticate only when the application session, the Oracle single sign-on session and the third-party session

have all become invalid.

Single Sign-On Technical Architecture

When an unauthenticated user attempts to access Oracle E-Business Suite Release 12.2, Oracle E-Business Suite Release 12.2 delegates user authentication to Oracle Access Manager, which in turn delegates to the third-party authentication mechanisms.

User Management

Oracle Directory Services and Third-Party LDAP Directories

- Oracle Directory Services can synchronize user information with a third-party LDAP server using the synchronization process.
- Oracle Directory Services includes tools to bulk migrate user between Oracle Directory Services and third-party LDAP server.

> **Additional Information:** Refer to *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* or *Oracle Fusion Middleware Administering Oracle Unified Directory* for more information.

Strategies for User Management

At the starting point of the deployment, the third-party LDAP server is the sole user repository. For users registered there who will need to access Oracle E-Business Suite, the single sign-on solution requires them to exist in Oracle Directory Services as well as in Oracle E-Business Suite Release 12.2.

Oracle recommends retaining the third-party LDAP directory as the primary source of truth for user information. Use the Oracle Directory Services synchronization solution to migrate users from the third-party LDAP directory into Oracle Directory Services, and then use the Oracle Directory Services provisioning solution to move users into Oracle E-Business Suite.

> **Important:** For pending users that are enabled in Oracle E-Business Suite after user creation, the IDENTITY_MODIFY event from E-Business Suite to Oracle Directory Services must be enabled.

Populating E-Business Suite with Third-Party LDAP Users

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

Creating New Users

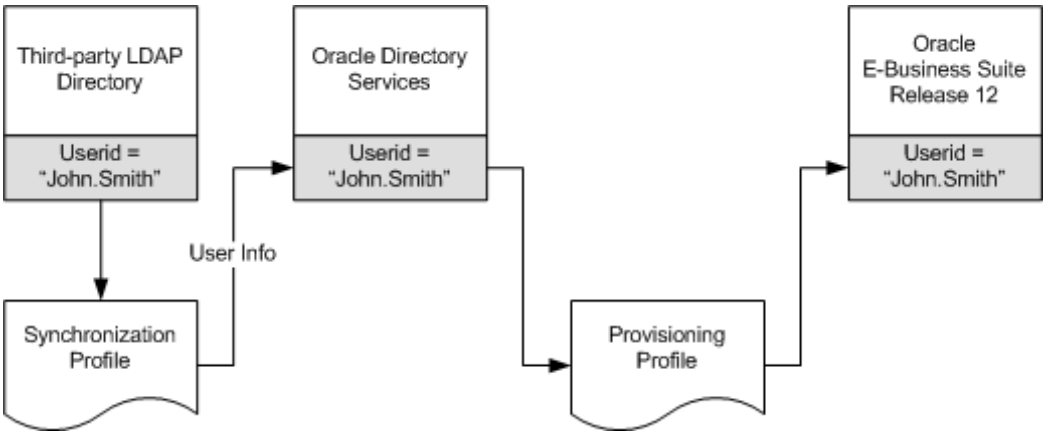
System administrators can create synchronization profiles to integrate Oracle Directory Services with the third-party LDAP directory, which results in:

- Creation of a new single sign-on account in the third-party LDAP directory automatically triggering the creation of a new single sign-on account in Oracle Directory Services.
- Ability to specify users to be synchronized, and which attributes of the users are to be created in Oracle Directory Services.
- Creation of a GUID attribute for each user created in Oracle Directory Services.

System administrators also create provisioning profiles to integrate Oracle E-Business Suite Release 12 with Oracle Directory Services, which results in:

- Creation of a new account in Oracle Directory Services automatically triggering the creation of a new application account in Oracle E-Business Suite Release 12.
- Ability to specify user attributes created in Oracle E-Business Suite.

Diagram of Using Synchronization Profiles to Integrate Oracle Directory Services with a Third-Party LDAP



Updating User Information (optional)

System administrators can configure synchronization profiles to synchronize some or all of the user attributes from the single sign-on account in the third-party LDAP directory into the single sign-on account in Oracle Directory Services when those attributes are modified.

System administrators can configure provisioning profiles to provision some or all of the user attributes from Oracle Directory Services into Oracle E-Business Suite when

those attributes are modified.

Terminating and End-Dating Users

Synchronization and provisioning profiles can also be used to configure the system such that terminating a user in the third-party LDAP directory also end-dates the user in Oracle E-Business Suite.

Password Management

Password management can, if desired, remain as it was before the integration. That is, user passwords can remain in the third-party LDAP; it is not necessary to duplicate them in Oracle Directory Services. Note that Oracle E-Business Suite will not store passwords for users provisioned from Oracle Directory Services.

- **End user tasks**: Most end users should use the methods provided by the third-party LDAP directory for password maintenance functions.
- **System administrator tasks**: To reset single sign-on passwords, an administrator should follow the methods provided by the third-party LDAP directory.
- **Password management policies**: User's password creation, modification and single sign-on login activities are subject to the third-party LDAP rules that govern how passwords are created and used.

Critical Implementation Decisions

Oracle Directory Services has a powerful and flexible set of configuration options. Most Oracle E-Business Suite system and security administrators will be able to use the default Oracle Directory Services configuration. Security administrators with advanced security requirements may choose to use alternate Oracle Directory Services configurations. For more information, refer to *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* or *Oracle Fusion Middleware Administering Oracle Unified Directory*.

1. Oracle E-Business Suite integration:
   - Identity management realm
   - DIT structure
   - The attribute chosen as the nickname attribute
2. Synchronization between Oracle Directory Services and third-party LDAP directory:
   - Identifying users who need to access Oracle E-Business Suite Release 12.2, and

must therefore be synchronized from the third-party LDAP directory to Oracle Directory Services.

- Which user attributes to synchronize from the third-party LDAP directory to Oracle Directory Services.

3. Provisioning between Oracle Directory Services and Oracle E-Business Suite:
   - Which attributes to provision during account creation.
   - Whether to provision user changes from Oracle Directory Services to Oracle E-Business Suite Release 12.2. If yes, which attributes to provision.
4. Single sign-on settings
5. Session timeouts for Oracle Access Manager, third-party single sign-on, and Oracle E-Business Suite Release 12.
6. Current third-party LDAP/single sign-on deployment information, including host, port, and administration account information.
7. Documentation from Oracle and third-party LDAP and single sign-on product vendors describing integration with Oracle Application Server 10g.

Implementation Instructions

1. Configure Oracle Access Manager to work with third-party authentication mechanism.
2. Replicate existing accounts that need to access Oracle E-Business Suite from third-party LDAP into Oracle Directory Services. Configure Oracle Directory Services and third-party LDAP synchronization process.
3. Migrate existing Oracle Directory Services users into Oracle E-Business Suite.
4. Set Oracle E-Business Suite profile options. The profile settings should be similar to that of the base scenario. Refer to Single Sign-On Profile Options, page 5-52 for details of all relevant profile options.

Variations On This Scenario

Variation of this scenario may have some of the following characteristics:

- Oracle E-Business Suite fresh install.
- Existing Oracle Access Manager and Oracle Directory Services infrastructure.

- No third-party authentication mechanism or third-party LDAP directory involved.

The major difference here is that the steps relating to third-party (non-Oracle) software can be ignored.

Deployment Scenario 3: Existing Oracle E-Business Suite Instance + Existing Third-Party Identity Management Solutions

This scenario describes a more complex deployment possibility, which may be required in some larger organizations.

Starting Point

- Oracle E-Business Suite Release 12.2 is in use, and has existing users populated in an up-to-date FND_USER repository.
- A third-party authentication mechanism is in use as a corporate single sign-on solution.
- A third-party LDAP directory in use as a corporate user directory.
- At the start of the implementation, a 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.

Architectural Requirements

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

Solution Outline

- Oracle Access Manager, Oracle E-Business Suite AccessGate, and Oracle Directory Services are used 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 authentication mechanism in use.
- 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 by using 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 third-party LDAP 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.

- *Optional*: User profile information in Oracle E-Business Suite can be kept synchronized with the information in the third-party LDAP directory.

Solution Details

The single sign-on, sign-off and session timeout processes in this deployment scenario are similar to that in Scenario 2, with one significant difference during sign-on. In the case where a user already has an account in the third-party LDAP directory and an account in Oracle E-Business Suite (with the same account name or a different account name), Oracle recommends the following approach:

- Migrate the third-party LDAP account into Oracle Directory Services through either the bulk migration tool (for existing accounts) or the synchronization process (for new accounts).

- Use the Link-on-the-Fly feature to link the single sign-on account in Oracle Directory Services with the applications account in Oracle E-Business Suite Release 12.2, by proceeding as follows:

  1. In the single sign-on handshake (described in the base scenario), Oracle Access Manager returns the GUID of the authenticated user to Oracle E-Business Suite.

  2. Oracle E-Business Suite then uses the GUID to try to locate the user's Oracle E-Business Suite application account.

  3. If it is the first time the user is accessing an Oracle E-Business Suite instance, no associated application account will be found, since the user's Oracle E-Business Suite account did not have the GUID information before the Oracle Access Manager integration took place.

  4. The user is directed to a Link Account screen for entry of the Oracle E-Business Suite user name and password.

- Once the application account information has been successfully verified, the user is redirected to the requested Oracle E-Business Suite page or the user's home page, as applicable. Additional logic is as follows:

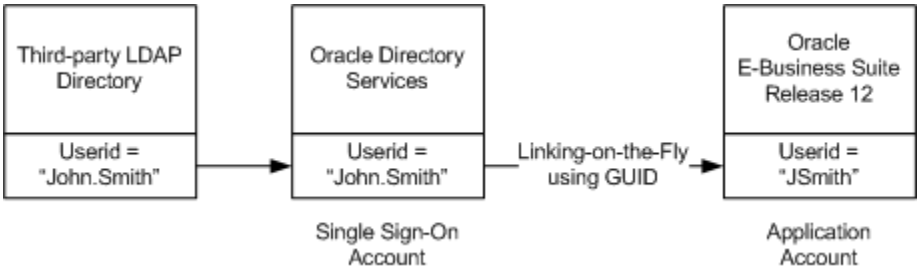
  1. The association between the single sign-on account and the application account (represented by the GUID) is retained.

  2. Oracle E-Business Suite will not redirect the user to the Link Account page on subsequent accesses.

3. If the application account information is not verified, the user is directed back to the Link Account page.

- This overall process is illustrated by the following diagram:

Deployment Scenario Flow



Advanced Option: In cases where users have accounts in both a third-party LDAP directory and Oracle E-Business Suite, it may sometimes be the case that all the LDAP account names are known to be identical to the Oracle E-Business Suite account names. In such cases, the value of the profile Applications SSO Auto Link User can be set to 'Y'. Subsequently, when Oracle E-Business Suite fails to locate an application account by GUID, it will try to locate one by the account name, and if successful it will then link the two accounts by GUID. The linking operation will be performed behind the scenes, and the user will not see the Link Account page. See Single Sign-On Profile Options, page 5-52 for more details.

User Management Options

The complexity of user management in this scenario lies mostly in the process of reconciling existing user data in the third-party LDAP and Oracle E-Business Suite. It is always necessary to synchronize the third-party LDAP data into Oracle Directory Services for any users who need to access Oracle E-Business Suite using single sign-on. The single sign-on accounts in Oracle Directory Services should be identical to the accounts in the third-party LDAP directory. No action is required for users whose details reside in the third-party LDAP and who do not need to access Oracle E-Business Suite.

For the rest of this discussion, it is assumed that all existing third-party LDAP users will need to access Oracle E-Business Suite, and that such users will therefore need to exist in Oracle Directory Services. Depending on the characteristics of the existing data and desired functionality, there are various possibilities.

Option 1: Require users always to have created an account in the third-party LDAP directory and an account in the Oracle E-Business Suite, using the user enrollment method provided by each system.

In this case, the LDAP accounts are migrated into Oracle Directory Services. The Oracle Directory Services accounts and the Oracle E-Business Suite accounts are linked

through the Link-on-the-Fly process described above (neither SUBSCRIPTION_ADD nor IDENTITY_ADD event are enabled in any provisioning profiles used).

Optionally, administrators can configure the synchronization and provisioning process so that changes in user attributes can be propagated:

- From the third-party LDAP directory into Oracle E-Business Suite using Oracle Directory Services
- From Oracle E-Business Suite into the third-party LDAP directory using Oracle Directory Services
- In both directions

The list of user attributes supported is currently limited, and listed later in Supported Attributes, page 5-93.

Option 2: Propagate new accounts from the third-party LDAP directory to Oracle E-Business Suite by using Oracle Directory Services (as described in Scenario 2).

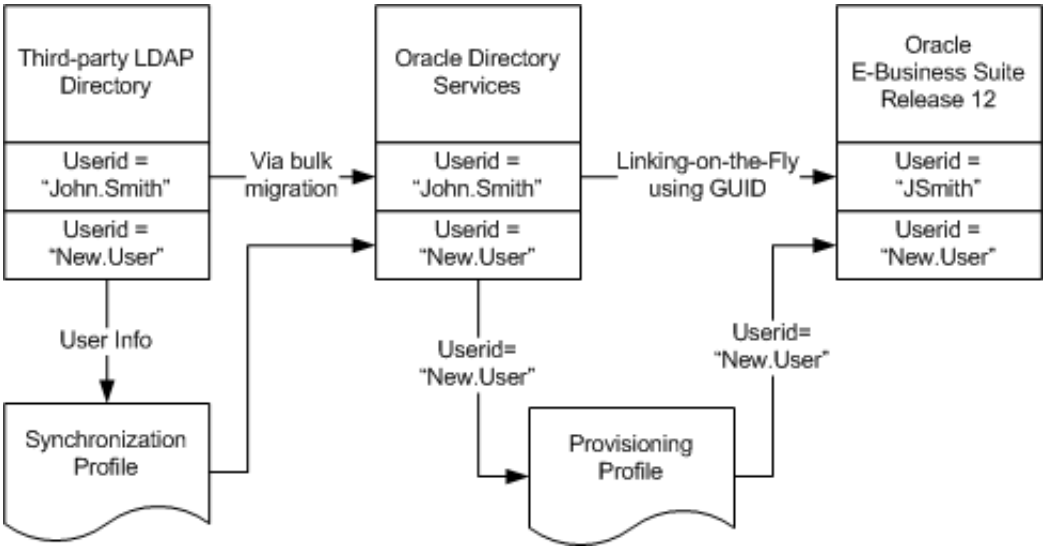
Existing accounts in LDAP and/or Oracle E-Business Suite will need to be reconciled. If a user has an existing account in the LDAP directory, and an existing account in Oracle E-Business Suite, the Link-on-the-Fly feature can be used to link the two accounts; no other action is required If a user has an existing account in Oracle E-Business Suite, but not in the third-party LDAP directory, an account must be created in the LDAP directory, and Link-on-the-Fly used to link the two accounts (this step needs to be performed before provisioning is configured).

If a user has an existing account in the third-party LDAP directory, but not in the Oracle E-Business Suite, an account must be created in Oracle E-Business Suite, and Link-on-the-Fly used to link the two accounts.

To eliminate the need to use the "Link Account" functionality for new users, new accounts can be propagated from the third-party LDAP directory to Oracle E-Business Suite through the Oracle Directory Services synchronization and provisioning process. This strategy also eliminates the need for new users to enroll multiple times. However, before enabling this process, system administrators must set up procedures to ensure that new account names created in the third-party LDAP directory will not conflict with any existing account names in Oracle E-Business Suite.

Optionally, administrators can configure the synchronization and provisioning process so that changes in user attributes can be propagated from the third-party LDAP directory into Oracle E-Business Suite using Oracle Directory Services.

User Management Options



Password Management

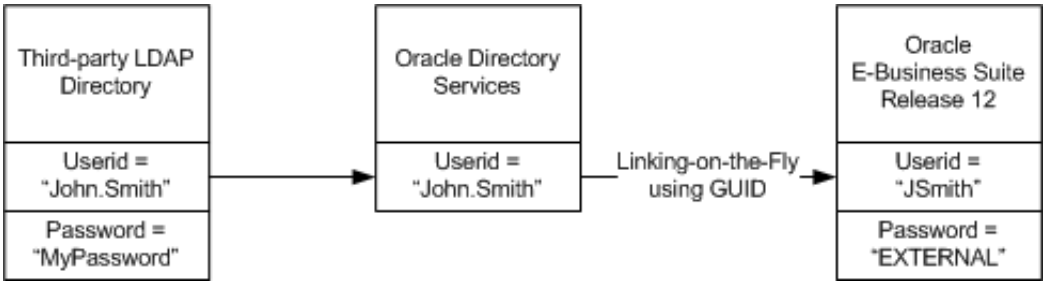
Once a single sign-on account in Oracle Directory Services is linked to an application account in Oracle E-Business Suite, the password for the application account in Oracle E-Business Suite is, as mentioned earlier, replaced with the reserved keyword "EXTERNAL." The password stored in the primary user directory for passwords is sufficient for authentication purposes.

Note that Oracle Access Manager delegates user authentication to the third-party single sign-on solution, which in turn authenticates users against the third-party LDAP directory. Users cannot gain access to Oracle E-Business Suite through AppsLocalLogin.jsp. As Oracle Directory Services passwords will be ignored, it is not advisable to retain any passwords in Oracle Directory Services.

> **Note:** If an SSO user's setting of APPS_SSO_LOCAL_LOGIN is changed to Local or Both (for local access), the user's password will need to be changed by an administrator.

The primary role of the third-party LDAP directory here can be represented as shown in the following diagram:

Diagram of the Role of the Third-Party LDAP Directory



Critical Implementation Decisions

1. Oracle Directory Services has a powerful and flexible set of configuration options. Most E-Business Suite system and security administrators will be able to use the default Oracle Directory Services configuration. Security administrators with advanced security requirements may choose to use alternate Oracle Directory Services configurations. Refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* or *Oracle Fusion Middleware Administering Oracle Unified Directory*.

   Items of particular importance to Oracle E-Business Suite integration are:

   - Identity management realm
   - DIT structure
   - The attribute chosen as the nickname attribute

2. Synchronization between Oracle Directory Services and third-party LDAP directory.

   Items of particular importance are:

   - Identifying users who need to access Oracle E-Business Suite Release 12.2 and who therefore need to be synchronized between the third-party LDAP directory and Oracle Directory Services
   - Which attributes to use to synchronize between Oracle Directory Services and the third-party LDAP directory

3. Which user management option described above to use.

4. Decisions related to single sign-on settings, especially session timeouts for:

   - Oracle Access Manager

- Third-party single sign-on components
- Oracle E-Business Suite Release 12.2

5. Current third-party LDAP and single sign-on deployment information, including host, port, and administration account information. For this, you may need to refer to documentation from Oracle and third-party LDAP and single sign-on product vendors describing integration with Oracle Access Manager.

Implementation Instructions

1. Depending on the user management options, develop a strategy to reconcile existing accounts in Oracle E-Business Suite Release 12.2 and the third-party LDAP directory.
2. Configure Oracle Access Manager to work with the third-party authentication mechanism.
3. Migrate existing third-party LDAP accounts to Oracle Directory Services, and configure synchronization between third-party LDAP and Oracle Directory Services.
4. Configure session timeout setting.
5. Set Oracle E-Business Suite profile options. Refer to Single Sign-On Profile Options, page 5-52 for further details of relevant profile options.

Variations On This Scenario

A variation of this scenario may have the following characteristics:

- Existing Oracle E-Business Suite Release 12.2 Installation
- Existing Oracle Access Manager and Oracle Directory Services infrastructure
- No third-party single authentication mechanism or third-party LDAP directory involved

The major difference here is that all steps relating to third-party (non-Oracle) software can be ignored.

Deployment Scenario 4: Multiple Oracle E-Business Suite Instances with Unique User Populations

Starting Point

- 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.

Architectural Requirements

This scenario applies to sites that have more than one Oracle E-Business Suite Release 12.2 instance in use, but no Oracle Access Manager infrastructure in place. The requirement is to enable Oracle Access Manager for the multiple Oracle E-Business Suite instances.

Solution Outline

- Oracle Access Manager, Oracle E-Business Suite AccessGate, and Oracle Directory Services are used 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, which 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.
- *Optional*: User profile information in Oracle E-Business Suite can be kept synchronized with the information in Oracle Directory Services.

Solution Details

The single sign-on architecture is the same as that described in the base scenario. In addition, the Link-on-the-Fly feature described in Scenario 3 may be used.

User Management Options

The options for user management in this scenario depend on the characteristics of existing user data in the multiple Oracle E-Business Suite instances.

Option 1: If one of the Oracle E-Business Suite instances is currently serving as the

source of truth for user information for all Oracle E-Business suite instances, it is possible to change this in a two-stage process. First, migrate the existing users from that Oracle E-Business Suite instance into Oracle Directory Services using the bulk migration tool, and then configure the provisioning process such that any further new users created in that Oracle E-Business Suite instance are automatically provisioned into Oracle Directory Services.

- Users who already have accounts on the other Oracle E-Business Suite instances will use the Link-on-the-Fly mechanism to link their single sign-on accounts to their application accounts on those instances.

- New users provisioned into Oracle Directory Services can be selectively provisioned into the other Oracle E-Business Suite instances.

Option 2: If none of the existing Oracle E-Business Suite instances is the primary source of truth for user information, it is possible to migrate the existing accounts in all Oracle E-Business Suite instances into Oracle Directory Services with the following restrictions on the existing data:

- No two users have the same account names across all Oracle E-Business Suite instances.

- If a user has accounts in multiple Oracle E-Business Suite instances, those accounts must be of the same account name.

After the migration, new users can be created from Oracle Directory Services, and then selectively provisioned into an Oracle E-Business suite instance.

Option 3: If the above options are not feasible, a deployment may choose not to rely on the provisioning process for creating accounts (no SUBSCRIPTION_ADD nor IDENTITY_ADD event enabled in provisioning profile). Every user who needs single sign-on access to an Oracle E-Business Suite is required to have created a single sign-on account in Oracle Directory Services, and an application account in that Oracle E-Business Suite Release 12.2 instance, by using the user enrollment method provided by each system. The Oracle Directory Services account and Oracle E-Business Suite account are linked through the Link-on-the-Fly process when the user accesses an Oracle E-Business instance for the first time.

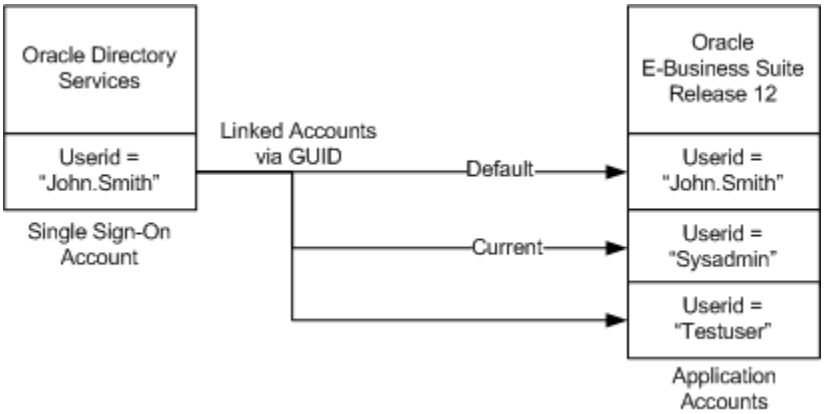
Advanced Features

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

In most cases, a user's single sign-on account in Oracle Directory Services will correspond to a single application account in Oracle E-Business Suite Release 12.2. However, there may be special cases where a user has a single sign-on account in Oracle Directory Services and multiple application accounts in Oracle E-Business Suite Release 12.2. In such a case, it is possible to associate a single sign-on account in Oracle

Directory Services with multiple application accounts in Oracle E-Business Suite Release 12.2:

Diagram of an Oracle Directory Services Single Sign-On Account Associated with Multiple Application Accounts



This feature can be enabled by system administrators by using a profile option (Applications SSO Allow Multiple Accounts). To utilize this feature, proceeds as follows:

1. Log in to Oracle E-Business Suite using a valid single sign-on account in Oracle Directory Services.

2. Once logged in, access the Single Sign-On Account Settings page by clicking **Account Settings** from the Preferences page.

3. To associate additional application accounts with an existing single sign-on account, choose Add Account and enter the new application account user name and password when prompted.

4. Verification of the new application account information will result in redirection back to the Single Sign-On Account Settings page, showing the newly linked account.

5. Failure to verify the new account information will result in redirection back to the Add Account page.

The first linked application account is marked as the default application account for the single sign-on account, and is the account the user will be logged into after Oracle single sign-on authentication. If required, the default account can be changed by making the appropriate selection on the Single Sign-On Account Settings page.

After logging into Oracle E-Business Suite using Oracle single sign-on, a user can view all currently linked application accounts using the Single Sign-On Account Settings page, and can, if desired, switch to another linked application account by selecting that account and clicking on **Make Current Account**. If this feature is disabled by the system

administrator, the **Add Account** button will not appear on the Single Sign-On Account Settings page and users will not be permitted to link multiple application accounts to their single sign-on account.

Only one single sign-on account in Oracle Directory Services may be linked to a given application account in Oracle E-Business Suite Release 12.2 at a time; simultaneous linking of multiple single sign-on accounts to a single application account is not supported.

The FND_SSO_UTIL package contains procedures for linking and unlinking users. For more information, see: FND_SSO_UTIL Procedures, page 5-96.

Time Zone Support

Oracle Access Manager and the Oracle E-Business Suite database machine system clocks should be accurate, and kept synchronized. If the clocks are inaccurate or out-of-sync, user provisioning flows may be affected.

Be aware of the following points:

- Oracle Access Manager converts all times to GMT. If the orclStartDate attribute is defaulted, it will pick the system date and convert it to GMT.
- The Oracle E-Business Suite database machine runs in the local time zone, so dates are also in the local time zone.
- When a user is provisioned from Oracle Directory Services, the dates are converted to the local time zone.

Switching User Back to Local Authentication

It may be necessary to switch the user management source of truth from Oracle Directory Services back to Oracle E-Business Suite for specific users. Credentials for these users will need to be switched back to being authenticated by FND_USER for local authentication. Special procedures to do this are necessary, because the FND User form as well as the User Preferences screen will not allow you to change the password once it has been set to "EXTERNAL."

To preserve the password and allow users to locally log in to Oracle E-Business Suite, follow these steps:

1. Ensure that the profile option Applications SSO Login Types (APPS_SSO_LOCAL_LOGIN) is set to either "LOCAL" or "BOTH" for users to whom you want to keep the local access.
2. Use the AFPASSWD utility or FNDCPASS utility to reset the user's password. The new password then needs to be emailed to the user.

For more information about the AFPASSWD and FNDCPASS utilities, refer to Basic

DBA Tasks in *Oracle E-Business Suite Maintenance Guide*.

Recommended Nickname (Login Attribute) Setting

The default nickname used for login is "uid", which can be verified in the Oracle Directory Services Delegated Administration Service Configuration screen, Attribute for Login Name field. "uid" corresponds to User Name in the Oracle Directory Services Manager UI.

Changing the nickname attribute is generally not recommended, but other unique attributes such as email address can be used in special circumstances. Oracle E-Business Suite currently supports setting of the nickname (login attribute) to either *uid* or *mail*.

The attribute set as the nickname in Oracle Directory Services is mapped to the FND_USER.USER_NAME column in the Oracle E-Business Suite database. If the nickname is changed in Oracle Directory Services, the Oracle E-Business Suite database must be restarted to force a refresh of the cached value.

Customizing Directory Information Tree (DIT) and Relative Distinguished Name (RDN)

Customizable Directory Information Trees (DIT) and Relative Distinguished Names (RDN) are supported for use with Oracle E-Business Suite single sign-on environments. Described further in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* and *Oracle Fusion Middleware Administering Oracle Unified Directory*, the following parameters can be defined at realm level:

- Name Attribute (NickNameAttribute)
- UserCreateBase: one or more DN where the user entries are located
- Attribute for RDN
- UserSearchBase: in the hierarchical path for all defined UserCreateBases, this is the location to start searching for users of a given user name

> **Caution:** Implementing the Custom DIT feature in an existing infrastructure is not recommended, as it may result in data corruption. If there is such a need, contact Oracle Support for details of how to migrate existing data safely.

The Custom DIT feature should not be confused with Multiple Realm support.

Custom DIT Configuration Steps

The Custom DIT feature requires the following configuration steps within Oracle Directory Services, Oracle Access Manager, and Oracle E-Business Suite.

See the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* or

Oracle Fusion Middleware Administering Oracle Unified Directory for more details.

In Oracle Directory Services

1. Create the new DIT structure.

2. Optionally, configure the CommonNameAttribute to be used for the RDN (the default is cn).

3. Specify a single UserSearchBase where all UserCreateBases can be located. This can be updated using one of the following methods:

   1. Using the ODSM user interface.

      For example:

      `cn=Common,cn=Products,cn=OracleContext,dc=example,dc=com`

      In the "Optional Attributes" section, locate the `orclCommonUserSearchBase` attribute and add the new search base.

      For example:

      `cn=new_repository,dc=example,dc=com`

   2. Using the `ldapmodify` command.

      For example:

      ```
      ldapmodify -h <host> -p <port> > -D "cn=orcladmin" -w
      <password> -f <full file path to ldif file>
      ```

      A sample ldif file is as follows:

      ```
      dn:cn=Common,cn=Products,cn=OracleContext,dc=example,dc=com
      changetype: modify
      add: orclCommonUserSearchBase
      orclCommonUserSearchBase:cn=new_repository,dc=example,dc=com
      ```

      > **Caution:** The current implementation supports only one UserSearchBase. Using more than one may result in incorrect operation.

4. Add access control for the new container. For details, see My Oracle Support Knowledge Document 1311294.1, *ORA-20001 and ORA-31202 When Creating a User in EBS With Custom DIT*.

In Oracle Access Manager

1. Log in to the Oracle Access Manager (OAM) console.

2. Navigate to **Configuration** >**User Identity Store** >**OID Identity Store** (or OUD Identity Store).

3. Update the user search base with the new DIT.

In Oracle E-Business Suite

1. Register the Oracle E-Business instance with the desired deployment template. Note that this feature is only relevant for the deployments provisioning users from Oracle E-Business Suite to Oracle Directory Services.

2. From the APPS account, run the API `fnd_oid_plug.setplugin` from SQL*Plus to configure Oracle E-Business Suite for use with the new user repository.

   For example:

   ```
   sql> fnd_oid_plug.setPlugin
   (default_user_repository=>'cn=new_repository,dc=example,dc=com');
   ```

   The Oracle Directory Services configuration attributes are now stored in Oracle E-Business Suite preferences.

   > **Note:** Any configuration changes in OID will require this API to be re-run so that the new values are picked up by Oracle E-Business Suite.

   The preference storing the create base can be confirmed using the following query from the Oracle E-Business Suite instance:

   ```
   select fnd_preference.get
   ('#INTERNAL','OID_CONF','CREATE_BASE') from dual;
   ```

3. Stop and restart the application tier processes.

4. Verify that the new users are successfully created and modified from Oracle E-Business Suite to Oracle Internet Directory or Oracle Unified Directory.

Now, when new users are created in Oracle E-Business Suite, they will also be created in the User Repository. This will have no impact to the propagation of users from Oracle Directory Services to Oracle E-Business Suite. Note, however, that the same "user" cannot be created in multiple user repositories.

If an error occurs, enable FND Logging and review the log output to get the error details. For example:

```
ERROR
------------------------
Unable to call fnd_ldap_wrapper.create_user due to the following reason:
ORA-20001: Unabled to call fnd_ldap_wrapper.create_user due to the
following reason:
An unexpected error occurred. Please contact your system administrator
```

In FND_LOG_MESSAGES, the following error is seen:

```
fnd.plsql.oid.fnd_ldap_user.create_user: 4 ORA-31202: DBMS_LDAP: LDAP
client/server error: Insufficient access
```

This error indicates that the access control was not added for this DIT.

Single Sign-On Profile Options

The logon process by which users are authorized to access Oracle E-Business Suite is significantly modified in an environment where Oracle Access Manager (and the associated Oracle E-Business Suite AccessGate) have been integrated. This section discusses the key changes, in particular the use of profile options.

Overview of Login Pages

In a standalone Oracle E-Business Suite environment, all users and system administrators connect by using Oracle E-Business Suite's AppsLogin page. This page redirects users to an Oracle E-Business Suite login page that authenticates their userid and password against the FND_USER table. Oracle E-Business Suite then determines the user's authorization by looking up the application responsibilities against entries in the FND_USER table.

In an environment where Oracle E-Business Suite has been integrated with Oracle Access Manager and Oracle Directory Services, the following points apply:

- End users connect to Oracle E-Business Suite using the AppsLogin page, which redirects them to the Oracle Access Manager login page. Oracle Access Manager authenticates the Oracle E-Business Suite user's userid and password against Oracle Directory Services, and redirects the user back to Oracle E-Business Suite, which then determines the user's authorizations by looking up application responsibilities against entries in the Oracle E-Business Suite FND_USER table.

- System administrators and other selected users connect to Oracle E-Business Suite using Oracle E-Business Suite's AppsLocalLogin page, which authenticates their userid and password against the FND_USER table. Oracle E-Business Suite then determines the user's authorizations by looking up application responsibilities against entries in the FND_USER table. Users in this special user population have their credentials authenticated locally in Oracle E-Business Suite instead of externally in Oracle Access Manager and Oracle Directory Services.

The login process is controlled by a group of Oracle E-Business Suite profile options, which are described in more detail below.

The key components involved in the login process are as follows.

AppsLogin

```
<http://[host]:[port]/OA_HTML/AppsLogin>
```

The login route is determined by the profile option "Applications SSO Type" (APPS_SSO). If the Oracle E-Business Suite instance is integrated with Oracle Access Manager, this should be set to "SSWA w/SSO." The user is redirected to the Oracle E-Business Suite AccessGate login page, and after entering his credentials (user name and password), he is authenticated against the LDAP server.

AppsLocalLogin

`<http://[host]:[port]/OA_HTML/AppsLocalLogin.jsp>`

The login route is determined by the profile option "Applications SSO Type" (APPS_SSO). If this site level profile is set to "SSWA", the user will be shown the local login page, and after entering his credentials (user name and password), he is authenticated against the Oracle E-Business Suite instance.

> **Note:** If APPS_SSO is set to SSWA, the user will be redirected to `AppsLocalLogin.jsp` regardless of whether or not OAM integration is in effect. When accessing `AppsLocalLogin.jsp`, the APPS_SSO profile is not used to determine the page to redirect to.

About the Lightweight Login Page

Starting with Oracle E-Business Suite Release 12.2.5, a lightweight login page is provided.

The lightweight login page consists of 4 components:

- HTML (`AppsLocalLogin.jsp`): includes the CSS and Javascript elements
- `login.css`: formats the HTML page
- `login.js`: Javascript to handle the page and the credentials posting
- LoginService: to attend REST service calls related to the login page

To customize the login page style, create a file called "custom-login.css" in the same directory as the `login.css` file with the same owner and protection. The `custom-login.css` file will automatically be appended to `login.css` when the login page is displayed.

> **Note:** Do not modify the `AppsLocalLogin.jsp`, `login.css`, or `login.js` files.

Login Page Display

The following items may be personalized. By default, all the items on the login page are displayed.

- User Name
- Password
- Login button

- Cancel button
- Login Assistance Link
- Register Here Link
- Accessibility
- Language Options

Customizing the Login Page

Oracle E-Business Suite Release 12.2.5 and Later

Suppress or Hide Elements on the Login Page

Use the profile FND_LOGIN_HIDE to enter a comma-separated list of elements to suppress or hide from the login page. Elements can be named by their DOM object ID or by the message the element displays. The ID must be preceded by the '#' or number sign.

For example, the following suppresses the display of the "Login Assistance" link and the copyright text at the bottom of the page:

```
FND_LOGIN_HIDE=#ForgotPasswordURL,FND_COPYRIGHT
```

Changing Colors and Backgrounds

Create a `custom-login.css` file to override attributes defined in the `login.css` file. Do not change the `login.css` or `login.js` files since they may be rewritten in the next patch.

For example, if you want to add an image to the disclaimer, add similar content to the `custom-login.css` file:

```
div[id="CopyrightBox"]::after { display: block; content: url('http:
//www.example.com/images/disclaimer.png'); }
```

Add/Override JavaScript

Create the file `custom-login.js`. This javascript file will be run when the page loads. Note that pages load asynchronously. Do not expect all HTML elements to be display at the same time.

Add/Remove/Modify HTML Elements Using JavaScript

Inside a `custom-login.js` file, create the function `document.afterLoad=function()`.

For example, if you want to add a custom disclaimer message at the bottom the login page for 12.2.5, you would add the following `custom-login.js`:

```
document.afterLoad=function()
{
var e = document.getElementById(C'opyrightBox');
e.innerHTML="<p> <em style='font-size: 1.5em' >JavaScript custom
Disclaimer</em> [custom-login.js]</p> ";
}
```

Note that this can be done only after the page load is completed.

Retain the Old Login Page from Oracle E-Business Suite Release 12.2.4

If you would like to retain the old login page from Oracle E-Business Suite Release 12.2.4 and earlier, create a copy of the old `AppsLocalLogin.jps` to `OldAppsLogin.jsp`, for example, and compile it. Then, set the profile value of APPS_LOCAL_LOGIN_URL to 'http://server:por/OA_HTML/OldAppsLogin.jsp'.

Oracle E-Business Suite Release 12.2.4 and Earlier

The login page for Oracle E-Business Suite Releases 12.2.4 and earlier is an Oracle Application Framework-based page. Administrators can personalize the page by performing the following the steps:

1. Set the profile FND_PERSONALIZATION_REGION_LINK_ENABLED to *Yes.*
2. Select the Functional Administrator responsibility.
3. Select the **Personalization** tab.
4. Enter the document path for the Local Login page definition.
5. Select a Region to customize.
6. This takes you to the Choose Personalization Context page: select **Apply**.
7. The personalization structure is displayed where an item can be selected and its properties changed.

Custom Login Pages

System Administrators can create custom login pages. The custom page will need to post to the servlet AuthenticateUser, which requires two attributes: user name and password. Once the user is successfully authenticated, the servlet will redirect the user to a destination defined in *requestUrl* or the default *APPSHOMEPAGE*. If the authentication fails, the servlet will redirect the user to the login page with the error message in the parameter *errCode*.

To deploy a custom login page:

1. Place the new servlet in the OA_HTML directory.
2. Create a new function (FND_FORM_FUNCTION) - the web_html value of this function should be populated with file name of your new login page. The function

code should begin with 'APPS_LOGIN'.

3. Assign this function to the APPS_LOGIN_DEFAULT menu. As this menu is already granted to all users (including guest), the grant flag is not needed.

4. Update the profile option APPS_LOGIN_FUNCTION with new function name. The drop-down for this profile will query only function codes starting with APPS_LOGIN.

5. Set the profile APPS_LOCAL_LOGIN_URL to point to the custom login page. Ensure that the page includes:
   - The javascript file "login.js"
   - A form containing id=login with inputs for `usernameField` and `passwordField`
   - A button with "onclick=submitCredentials()"

> **Note:** Custom login pages do not necessarily have all of the same functions as the default login page (e.g., change language, translated error message display).

CRMLogin Servlet and jtflogin.jsp

```
<http://[host]:[port]/oa_servlets/CRMLogin.jsp>
http://[host]:[port]/OA_HTML/jtflogin.jsp
```

There is a new recommended login flow for the CRM System Administrator Console. You can use the servlet CRMLogin to log in. The servlet checks whether your system is SSO-enabled, and directs you to the appropriate login page. The old login page, `jtflogin.jsp`, is still supported, but is only recommended in cases where `jtflogin.jsp` has been customized.

Oracle Applications Manager Login

```
http://[host]:[port]/servlets/weboam/oam/oamLogin
```

> **Important:** Here, "oam" refers to Oracle Applications Manager, **not** Oracle Access Manager.

You will be prompted for the Oracle E-Business Suite user account and password. Log in to an account that has System Administrator and Self-Service System Administrator responsibilities. Upon successful login, the Oracle Applications Manager Console will show the Oracle E-Business Suite system to which you have connected.

Profiles and Profile Categories

The login process is determined by a group of Oracle E-Business Suite profile options, which are divided into several categories and described below. The major components

involved in the logon process are as follows.

Profiles for Login and Logout

The profiles described in this category are all related to the login and logout process.

Applications SSO Type (APPS_SSO)

Features of this profile:

- Available at site level (cannot be set for individual servers or users). As of Release 12.2.6, this may also be set at the server level.
- Updatable only by system administrators
- Defined by the lookup type 'APPS_SSO_TYPE'
- Has a default value of 'SSWA'

This profile determines the overall user login and authentication experience, as follows:

Applications SSO Type Profile Values

Profile Value	Login Using	Authentication	User Directory	Integration Model	Requires	Home Page
SSWA w/SSO	OAM login page	Oracle Access Manager	Oracle Directory Services	Oracle E-Business Suite is partner application to Oracle SSO	Oracle E-Business Suite AccessGate installed into Oracle E-Business Suite instance	Set by APPLICATIONS_HOME_PAGE profile

Profile Value	Login Using	Authentication	User Directory	Integration Model	Requires	Home Page
Portal w/SSO	OAM login page	Oracle Access Manager	Oracle Directory Services	Oracle E-Business Suite is a partner application to SSO	Oracle E-Business Suite AccessGate installed into Oracle E-Business Suite instance	Portal home page
SSWA	Oracle E-Business Suite login page	Oracle E-Business Suite	FND_USER	N/A	N/A	Set by APPLICATIONS_HOME_PAGE profile

Additional Information: In the above table, Oracle Directory Services = the LDAP directory with which Oracle E-Business Suite is integrated; OAM = Oracle Access Manager; SSWA = Self-Service Web Applications.

Self-Service Personal Home Page Mode (APPLICATIONS_HOME_PAGE)

This profile determines the default home page for the application, which is the first page a user sees after logging into Oracle E-Business Suite.

Note: Prior to Release 12.2.9, the profile option APPLICATIONS_HOME_PAGE determines the look-and-feel of the Oracle Self-Service Applications Personal Home Page. With the change to use Masonry, the user preference set in the Settings > Preferences page takes precedence over the profile option value. The values set in this page for both home page and icon style are stored in the FND_USER_PREFERENCES table. If no value is set here, the value from the APPLICATIONS_HOME_PAGE profile option is used.

Features of this profile:

- Available at site and user level (can be set for individual users)
- System administrators can change setting at both Site and user levels

- End users can change this from user level profiles
- Default value is 'Framework only'

> **Note:** If an end user changes the value for this profile option, that value overrides administrative-level personalization for the home page. In this case, those administrative-level personalizations will not be displayed for that user.

Features of this profile:

Features of the Self-Service Personal Home Page Mode Profile

Profile Value	Description
Framework Only	Displays the Home page from Release 12.2.3 and earlier, based on the value of profile option FND: Disable Configurable Home Page.
Framework Tree	Displays the Home page from Release 12.2.3 and earlier, based on the value of profile option FND: Disable Configurable Home Page.
Framework Simplified	Displays the Simple Home page from Release 12.2.4 and later.
None	Do not use a personal home page.

FND: Disable Configurable Home Page

This profile accepts a value of False or True to determine whether to display the Configurable Home page with the Tree-based Navigator or Home page with the flat list Navigator, respectively, when the Self Service Personal Home Page Mode profile is set to Framework Only or Framework Tree.

> **Note:** The combination of values set for the Self-Service Personal Home Page Mode and FND: Disable Configurable Home Page profile options affect the appearance of the home page. For details on the behavior that result from the various profile option combinations, see the "Home Page Profile Options" section of the *Oracle Application Framework Developer's Guide*, available from My Oracle Support Knowledge Document 1315485.1.

Applications Local Login URL (APPS_LOCAL_LOGIN_URL)

This profile specifies which login page is used to perform local access to Oracle E-Business Suite. When the 'Applications SSO type' profile is set to 'SSWA', the application login servlet (AppsLogin) will redirect a user to the login page specified by this profile.

Features of this profile:

- Available at site level only (cannot be set for individual users)
- Updatable only by system administrators
- Default value is 'AppsLocalLogin.jsp'

Applications Portal (APPS_PORTAL)

This profile is used to specify Oracle Portal-related settings.

Features of this profile:

- Available at site level only (cannot be set for individual users)
- Updatable only by system administrators
- Defines the portal entry page

Applications Post-Logout URL (APPS_SSO_POSTLOGOUT_HOME_URL)

This profile can be used to specify where the user should be redirected after logging out of the Oracle E-Business Suite instance. Profile changes take effect for newly created sessions only.

Features of this profile:

- Available at site and user level
- Default value is NULL
- May be any valid URL

> **Note:** Product groups may programmatically set the post-logout URL, overriding any site or user level profile settings.

Profiles for Linking Accounts

The profile options described in this category control how Oracle E-Business Suite user accounts are linked to single sign-on accounts.

Applications SSO Auto Link User (APPS_SSO_AUTO_LINK_USER)

This profile determines whether Oracle E-Business Suite Release 12.2 will automatically link an authenticated single sign-on account to an application account of the same account name, without prompting the user for authentication information for the application account during login.

Features of this profile:

- Available at site level only (cannot be set for individual users)
- Updatable only by system administrators
- Has possible values of:
  - Enabled - Allow auto link
  - Disabled - Do not allow auto link (the default)
  - Create User and Link - To create and link user on-demand

When automatic linking is enabled for users, they must meet two criteria: have the same name as the SSO user, and a USER_GUID of null or 1. FND Users with a different name, or with a USER_GUID that is not null and not 1, cannot be linked in this way.

> **Note:** As the user with GUID=1 cannot be linked on the fly, the only way to link this user is with APPS_SSO_AUTO_LINK_USER.

Applications SSO Link Same Names (APPS_SSO_LINK_SAME_NAMES)

This profile indicates whether the Oracle E-Business Suite Release 12.2 instance should link a newly-created Oracle E-Business Suite user to an existing Oracle Directory Services account with the same name.

- Available at site level only (cannot be set for individual users)
- Updatable only by system administrators
- Has possible values of:
  - Enabled - Link users with the same user name
  - Disabled - Do not link users with the same user name

Applications SSO Allow Multiple Accounts (APPS_SSO_ALLOW_MULTIPLE_ACCOUNTS)

This profile indicates whether the Oracle E-Business Suite Release 12.2 instance allows linking of one Oracle Directory Services user to multiple Oracle E-Business Suite user accounts.

Features of this profile:

- Available at site level only (cannot be set for individual users)
- Updatable only by system administrators
- Has possible values of:
  - 'Y' - Allow multiple accounts to be linked
  - 'N' - Do not allow multiple accounts to be linked (the default)

The Link additional account operation uses this profile, which has the following implications:

- If the APPS_SSO_ALLOW_MULTIPLE_ACCOUNTS profile is set to 'Y' in the Single Sign-On Account Settings page (accessible from the User Preferences page), the **Add Account** button will be shown.
- If the profile is set to the default value of 'N', the **Add Account** button will not be shown, and the Link account page will therefore not permit linking of multiple accounts.

Profiles for Password Settings

The profile options in this category specify how passwords are managed in a single sign-on Oracle E-Business Suite environment.

Applications SSO Login Types (APPS_SSO_LOCAL_LOGIN)

Features of this profile:

- Available at both site and user level (can be set for individual users)
- Updatable only by system administrators
- Determines whether a user's password is managed:
  - Externally in Oracle Directory Services
  - Locally in Oracle E-Business Suite
  - In both Oracle Directory Services and Oracle E-Business Suite

Valid values are defined in the Lookup Type, FND_SSO_LOCAL_LOGIN:

- **SSO** - Login is only allowed through single sign-on. The password is set to 'EXTERNAL' after a single sign-on account and an application account are linked.
- **LOCAL** - Login is only allowed through Oracle E-Business Suite local login.

Passwords must be retained in the Oracle E-Business Suite and the account cannot be linked to any Oracle Directory Services user.

- **BOTH** - Login can be through both single sign-on and Oracle E-Business Suite. Since changes to the Oracle E-Business Suite password can be synchronized to Oracle Directory Services, but not vice versa, a user's single sign-on password will not necessarily be synchronized with his Oracle E-Business Suite password.

The default site level value is "BOTH". The user level value, applicable for example to the `SYSADMIN` and `GUEST` accounts, is set to "LOCAL".

The `SYSADMIN` and `GUEST` user profile options should not be changed. The `SYSADMIN` user is a standard account that can only be used for local login, and cannot be used to log in using single sign-on. Once a password is set to "EXTERNAL" Oracle E-Business Suite, it is no longer possible to use the original password to log in locally. For the password to be changed if the profile is updated to allow LOCAL access, the AFPASSWD utility or FNDCPASS utility will need to be run by a system administrator.

> **Important:** Regardless of whether the user credentials are correct, a LOCAL user cannot be linked on the fly, and the linking page will display the error: *FND-9921: Unable to link account. This E-Business Suite user account is marked as a local account*. The user can then choose to enter a different (non-local) account to link to.

For information on using the FND_SSO_UTIL procedure to set this profile, see: FND_SSO_UTIL Procedures, page 5-96.

For more information about the AFPASSWD and FNDCPASS utilities, refer to the "Basic DBA Tasks" chapter of the *Oracle E-Business Suite Maintenance Guide*.

Applications Local Change Password URL (APPS_LOCAL_CHANGE_PWD_URL)

This profile stores the location of the page where Self-Service users can change their Oracle E-Business Suite password. The page specified should only allow the password to be changed by a user whose APPS_SSO_LOCAL_LOGIN profile has the value of either "BOTH" or "LOCAL" (that is, not "SSO").

> **Note:** For 'SSO' and 'Both' users an API is used to determine whether the password can be changed locally, or if the APPS_SSO_CHANGE_PWD URL should be used. The criteria are whether the password can be synchronized to OID.

Features of this profile:

- Available at site level only (cannot be set for individual users)
- Updatable only by system administrators

- Default value is 'AppsChangePassword.jsp'

Applications SSO Change Password URL (APPS_SSO_CHANGE_PWD_URL)

This profile points to the LDAP self-service user interface for password changes. When an Oracle E-Business Suite Self-Service change password page determines that a user's password in stored in LDAP, it can redirect the user to the location stored in this profile. For example, the password may be stored in Oracle Identity Management.

Features of this profile:

- Available at site level only (cannot be set for individual users)
- Updatable only by system administrators

Profiles for Provisioning Settings

The profile options in this category determine how provisioning (automatic updating of user accounts) is carried out in a single sign-on Oracle E-Business Suite environment.

Applications SSO LDAP Synchronization (APPS_SSO_LDAP_SYNC)

This profile determines whether provisioning is enabled for a particular FND_USER account. User information associated with an FND_USER account will be provisioned with Oracle Directory Services only if the APPS_SSO_LDAP_SYNC profile of the user is set to 'Y'.

Features of this profile:

- Available at site and user level (can be set for individual users)
- System administrators can change setting at both site and user levels
- End users can change this from user level profiles.
- Default site level value is 'Y'
- User level values for `SYSADMIN` and `GUEST` accounts are set to 'N'

The site level value is provided to obviate the need for every user to define a user level value, and has the following important characteristics:

- Setting the site level value (to 'Y' or 'N') does not globally enable (or disable) provisioning.
- Since provisioning with Oracle Directory Services is the most common deployment scenario, this profile is shipped with a default site level value of 'Y'.
- For any user accounts that are not to be provisioned, this profile should be overridden with a user level value of 'N'.

- To provision users from FND to Oracle Directory Services, APPS_SSO_LDAP_SYNC needs to be enabled and the Oracle Directory Services provisioning profile set.

- If an existing user's APPS_SSO_LOCAL_LOGIN profile has "LOCAL" as the value, the user modifications are *not* provisioned, regardless of this profile value. Profile APPS_SSO_LOCAL_LOGIN has higher precedence than APPS_SSO_LDAP_SYNC at user level.

  Important: Linking a single enterprise user account to multiple Oracle E-Business Suite (FND_USER) user accounts can have undesirable consequences, such as data from one application overwriting data from another. Therefore, after the first FND_USER account is linked, all accounts subsequently linked to the same enterprise account will have the APPS_SSO_LDAP_SYNC user level profile value set to 'N'. Users who still wish to change the user level value of this profile can do so by using the Single Sign-On Account Settings page.

For information on using the FND_SSO_UTIL procedure to set this profile, see: FND_SSO_UTIL Procedures, page 5-96.

Applications SSO Enable OID Identity Add Event (APPS_SSO_OID_IDENTITY)

This profile determines whether users created in Oracle Directory Services are automatically created in Oracle E-Business Suite and subscribed to the given Oracle E-Business Suite instance. You can enable this profile to allow the automatic subscriptions for users created in Oracle Directory Services.

Features of this profile:

- Available at site level only (avoids the need for every user to define a user level value)

- System administrators can change setting at site level

- Default site level value is 'Disabled'

The default site level value of 'Disabled' means that users created in Oracle Directory Services will not be automatically created in Oracle E-Business Suite. The reason for this is that significant numbers of users from different sources may be created in Oracle Directory Services quite rapidly, and typically not all will also need to be created in Oracle E-Business Suite.

When the profile 'Applications SSO Enable OID Identity Add Event' value is set to 'Enabled', users created in Oracle Directory Services are automatically both created in Oracle E-Business Suite and subscribed to the Oracle E-Business Suite instance.

Applications SSO User Creation And Updating Allowed (APPS_SSO_USER_CREATE_UPDATE)

This profile is for Oracle internal use only.

Configuring Directory Integration Platform Provisioning Templates

This section describes how to configure an Oracle E-Business Suite Release 12.2 instance as a provisioning integrated application with Oracle Access Manager. The goal is to keep user information synchronized between Oracle Directory Services and Oracle E-Business Suite Release 12.

Configure and Create a Provisioning Profile

Bidirectional provisioning between Oracle E-Business Suite and Oracle Directory Services is built around the Oracle Directory Integration Platform, as described further in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* or *Oracle Fusion Middleware Administering Oracle Unified Directory*.

A key feature of this solution is the provisioning integration service, which enables automatic provisioning (updating between the systems) of account creation or changes of user attributes. The provisioning process between each Oracle E-Business Suite instance and Oracle Directory Services is controlled by a provisioning profile.

When changes are made in Oracle Directory Services that match an application's provisioning profile event subscription criteria, the Provisioning Integration Service is the agent that sends the relevant new data to that application. Going in the other direction, the Provisioning Integration Service filters changes coming from an application (according to the application's provisioning profile's permitted events criteria), and transmits applicable ones to Oracle Directory Services.

One of the advantages of this solution is a high level of flexibility at deployment time, i. e. the provisioning profile is highly customizable. Configuration of the profile is carried out by either using the `oidprovtool`, or by instantiating an LDIF template file that contains the requisite values for the particular deployment.

Profile Creation Prerequisites

Before a profile can be created, the relevant Oracle E-Business Suite instance must be registered with Oracle Directory Services. This involves creating a unique application identity for the instance in Oracle Directory Services.

Oracle E-Business Suite instances are created at the following location in the directory information tree (DIT): "cn=E-Business,cn=Products,cn=OracleContext, <Identity Management Realm>"

The created application identity (combination of dn and password) also needs to be stored in Oracle E-Business Suite. Note that the registered application identity and password can be used by the application administrator to connect to Oracle Directory Services for certain tasks, such as querying the provisioned profile details between this

application instance and Oracle Directory Services.

Provisioning Profiles - Configuring Provisioning Events

CREATION, MODIFICATION, and DELETION events can be enabled or disabled individually. Four event types are currently used:

- SUBSCRIPTION_ADD
- IDENTITY_ADD
- IDENTITY_MODIFY
- IDENTITY_DELETE

Each of these is described below:

SUBSCRIPTION_ADD

This event is generated by either Oracle Directory Services or Oracle E-Business Suite Release 12.

Oracle Directory Services maintains a subscription list for each Oracle E-Business instance that has registered with Oracle Directory Services. The subscription list maintains a list of all single sign-on user accounts that need to access the associated Oracle E-Business Suite instance.

- Oracle Directory Services and the associated Oracle E-Business Suite instance jointly maintain the accuracy of the subscription list.
- When a single sign-on account is created in Oracle Directory Services, and subsequently added to the subscription list of an Oracle E-Business Suite instance (see Manual Subscription Management With Provsubtool, page 5-76 for how this is done), a SUBSCRIPTION_ADD event is generated in Oracle Directory Services. If this event is enabled in the Oracle Directory Services to Oracle E-Business Suite direction, a new application account will be created and linked to the single sign-on account.
- When Oracle Directory Services receives an IDENTITY_ADD event (see below) from an Oracle E-Business Suite instance, it adds the user to the subscription list of that Oracle E-Business Suite instance.
- When Link-on-the-Fly is performed on an Oracle E-Business Suite Release 12 instance, the Oracle E-Business Suite instance will send a SUBSCRIPTION_ADD event to Oracle Directory Services.
- When an IDENTITY_MODIFY (see below) event is generated in Oracle Directory Services, Oracle Directory Services will check the subscription lists of all registered Oracle E-Business Suite Release 12 instances, and only send the event to an Oracle E-Business Release 12 instance if the modified user appears on its subscription list.

IDENTITY_ADD

This event is generated by either Oracle E-Business Suite or Oracle Directory Services when a new user is created. If this event is enabled from Oracle E-Business Suite to Oracle Directory Services direction, after Oracle Directory Services receives this event, it will create an Oracle single sign-on account in Oracle Directory Services and add the account to the subscription list of that Oracle E-Business Suite Release 12 instance. The other way, if this event is enabled from Oracle Directory Services to E-Business Suite and profile Applications SSO Enable OID Identity Add Event is 'Enabled', it has the same affect as SUBSCRIPTION_ADD event generated by Oracle Directory Services.

IDENTITY_MODIFY

This event is generated by either Oracle Directory Services or Oracle E-Business Suite when a user account is modified. If this event is enabled in either direction, the receiving system will apply the modification to the account on that system.

IDENTITY_DELETE

This event is generated by Oracle Directory Services when an Oracle single sign-on account is deleted. If this event is enabled from the Oracle Directory Services to Oracle E-Business Suite direction, after an Oracle E-Business Suite Release 12 instance receives this event, it will end-date the application account linked to the Oracle single sign-on account.

Provisioning Direction

Each event can be enabled in:

- One direction:
  - From Oracle Directory Services to Oracle E-Business Suite only
  - From Oracle E-Business Suite to Oracle Directory Services only
- Both directions:
  - From Oracle Directory Services to Oracle E-Business Suite
  - From Oracle E-Business Suite to Oracle Directory Services

Attribute List

For each direction, and each type of event, the list of provisioned attributes can be customized as required (removing an attribute from the attribute list would disable sending that attribute). The Supported Attributes, page 5-93 section lists the attributes that are currently supported for each direction, and also as the mapping between Oracle Directory Services attributes and application table and column names.

Polling Interval

By default, Oracle Directory Services sends out provisioning events every 60 seconds; this value can be increased or decreased by using oidprovtool, or by editing the

`orclodipprofileschedule` attribute value in the provisioning template (see below). The polling interval should be set with caution; provisioning that is not frequent enough for site activity may have an impact on operations, while provisioning that is more frequent than necessary will result in needless network traffic.

Creating a Profile

Once the values of the configurable variables for a profile have been decided, there are two methods available to create the profile in Oracle Directory Services. The first is `oidProvTool` (see the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* or *Oracle Fusion Middleware Administering Oracle Unified Directory* for more information). The second option is to instantiate an LDIF template, which captures the configuration choices. The instantiated templates can then be loaded into Oracle Directory Services using the `ldapmodify` command. The template method is described in detail below.

Creating a Profile From a Provisioning Template

Creating the provisioning profile consists of the following steps:

1. Create a suitable template based on deployment choices. The sample templates shipped can be used as examples and starting points.
2. Instantiate the template with deployment specific values, to generate an LDIF file.
3. Load the LDIF file into Oracle Directory Services.

Once the LDIF file is loaded, Oracle Directory Services will start sending and polling provisioning events to and from the Oracle E-Business Suite instance for which the profile was created. It takes the provisioning service approximately two minutes to detect that a new profile has been added or an existing one has changed. The new or updated profile is then read by the service.

Four types of provisioning are provided by the registration utility:

- **BiDirectional Provisioning**: Set by specifying "-provisiontype=1" as a command line argument during Oracle Directory Services registration. This is the default provisioning type set by the registration utility.
- **InBound Provisioning**: Set by specifying "-provisiontype=2" as a command line argument during Oracle Directory Services registration
- **OutBound Provisioning**: Set by specifying "-provisiontype=3" as a command line argument during Oracle Directory Services registration.
- **BiDiNoCreation Provisioning**: Set by specifying "-provisiontype=4" as a command line argument during Oracle Directory Services registration.

To decide on the right template to use, an Oracle E-Business Suite administrator needs to determine the direction or directions of provisioning, and which provisioning events

need to be enabled in each direction. The deployment scenarios discussed in this section may be used as a reference.

For example, if the Oracle E-Business Suite instance only needs to send events to Oracle Directory Services, then an INBOUND provisioning profile should be created. If the Oracle E-Business Suite instance only needs to receive provisioning events from Oracle Directory Services, then an OUTBOUND profile should be created.

If provisioning events may need to be sent in both directions, a bidirectional profile (BOTH) should be created.

> **Note:** Oracle recommends using the base provisioning profile templates provided with Oracle E-Business Suite. Best-efforts support will be provided for customizations to the standard provisioning profile templates. Customers may wish to engage Oracle Consulting for assistance with specific customization requirements and issues.

Administering the Provisioning Process

The monitoring and other administration tasks for the provisioning process are normally performed by Oracle Directory Services system administrators. Refer to the *Oracle Internet Directory Release Administrator's Guide* for more details.

Each of the following sections cover topics related to Oracle Directory Services and Oracle E-Business Suite.

Maintaining DIP Server Log Files (Oracle Directory Services)

The main DIP log file is located in the `$ORACLE_HOME/ldap/log/odisrv<instance number>.log` directory. The <instance number> is a unique integer id, e.g. 1, assigned by a system administrator when specifying the instance parameter as part of the `oidctl` command line used to start the DIP server.

The provisioning profile logs are located in the `$ORACLE_HOME/ldap/odi/log directory`. Each log file name is of the form: `<ApplicationName>_<RealmName>_[I/E].[trc/aud]`.

Where:

- I = INBOUND provisioning event (from Oracle E-Business Suite to Oracle Directory Services)
- E = OUTBOUND provisioning event (from Oracle Directory Services to Oracle E-Business Suite)
- .trc = Trace file, which grows until the file size is approximately 10MB. When the maximum file size is reached, the current trace file is backed up (and a timestamp

appended) and a new trace file started. All old trace files are kept in the same directory.

- .aud = Audit file, which records all the events from the time the profile was created and therefore grows continually. This file consequently needs to be archived periodically. The system administrator needs institute a policy to back up and archive audit files. This will involve temporarily disabling the profile, archiving the audit file, then re-enabling the profile. If archiving is not required, the old audit file can simply be deleted.

  Additional Information: For more information, refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* or *Oracle Fusion Middleware Administering Oracle Unified Directory* for more details.

Enabling or Disabling a Profile (Oracle Directory Services)

To enable or disable a profile, use `manageProvProfiles` if the 11.1.1.9.0 stack is installed. The `oidProvTool` utility is to be used on previous release versions, prior to 11.1.1.9.0, although the utility is still delivered in 11.1.1.9.0 for backwards compatibility.

Refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* or *Oracle Fusion Middleware Administering Oracle Unified Directory* for usage of this tool.

Changing Profile Characteristics in an Existing Deployment (Oracle Directory Services)

If any properties of the provisioning profile are to be changed, the following steps must be performed.

For Oracle Internet Directory 11.1.1.9 (and Later) or Oracle Unified Directory:

1. Delete the existing profile using `manageProvProfiles`.
2. Use `manageProvProfiles` to create a new profile that suites the current requirements.

For Oracle Internet Directory Prior to 11.1.1.9:

1. Delete the existing profile, using `oidProvTool`.
2. Use `oidProvTool` to create a new profile that suits the current requirements.

The DIP server may take approximately two minutes to detect changes to the provisioning profile entries, that is, read the new profile configuration entry and then begin processing events based on the new configuration.

Creating Custom Workflow Subscriptions (Oracle E-Business Suite)

Customization of data synchronized between Oracle Directory Services and the Oracle E-Business Suite can be achieved by creating custom Workflow Business Event Subscriptions.

The required steps are:

1. Create the procedure that creates or updates the desired attributes. See example code below.

2. Create a new subscription for the relevant Workflow Business Event. Listed below are the Business Events provided, and how they are used:

   - **oracle.apps.global.user.change** - this event is raised whenever a FND_USER is updated by any source.

   - **oracle.apps.fnd.identity.add** - this event is raised whenever the Oracle E-Business Suite instance receives an IDENTITY_ADD event from Oracle Directory Services, such as when a new user is created in Oracle Directory Services.

   - **oracle.apps.fnd.identity.modify** - this event is raised whenever the Oracle E-Business Suite instance receives an IDENTITY_MODIFY event from Oracle Directory Services, such as when a user is updated in Oracle Directory Services.

   - **oracle.apps.fnd.identity.delete** - this event is raised whenever the Oracle E-Business Suite instance receives an IDENTITY_DELETE event from Oracle Directory Services, such as when a user is deleted from Oracle Directory Services.

   - **oracle.apps.fnd.subscription.add** - this event is raised whenever the Oracle E-Business Suite instance receives a SUBSCRIPTION_ADD event from Oracle Directory Services, such as when a user added to the subscription list in Oracle Directory Services.

   - **oracle.apps.fnd.subscription.delete** - this event is raised whenever the Oracle E-Business Suite instance receives a SUBSCRIPTION_DELETE event from Oracle Directory Services, such as when a user is deleted from the subscription list in Oracle Directory Services. Currently, this subscription does nothing in Oracle E-Business Suite. Administrators may customize this behavior by adding their own subscriptions.

   - **oracle.apps.fnd.ondemand.create** - this event is raised when a user is created on demand from SSO.

Example code for a custom Workflow subscription rule function

```
create or replace package custom_update_user AS
  function disable_fnd_user (p_subscription_guid   in   raw,
                             p_event   in out nocopy wf_event_t)
return varchar2;
end custom_update_user;


create or replace package body custom_update_user as

function disable_fnd_user (p_subscription_guid in  raw,
                         p_event   in out nocopy wf_event_t)
return varchar2 is

l_event_name          varchar2(256);
l_event_key           varchar2(256);
l_change_source       varchar2(256);
l_change_source       varchar2(256);
l_orcl_guid           fnd_user.user_guid%type;
l_ent_type            varchar2(256);
l_oid_user_enabled    boolean;
l_end_date            date;

if (p_event.GetValueForParameter('CHANGE_SOURCE') = 'OID') then
        l_event_key := p_event.GetEventKey();
        l_ent_type := wf_entity_mgr.get_entity_type(p_event.
GetEventName());
        l_orcl_guid      := wf_entity_mgr.get_attribute_value
(l_ent_type, l_event_key, 'ORCLGUID');
        l_end_date := wf_entity_mgr.get_attribute_value(l_ent_type,
l_event_key, 'ORCLACTIVEENDDATE');
     if (l_end_date <= sysdate) then
           fnd_user_pkg.DisableUser(username => l_event_key);
     end if;
end if;
        return(wf_rule.default_rule(p_subscription_guid, p_event));

exception when others
then
      return(wf_rule.error_rule(p_subscription_guid, p_event));
end disable_fnd_user;

end custom_update_user;
```

Customizing SSO Workflow Business Events (Oracle E-Business Suite)

Oracle Directory Services provisioning events are processed in Oracle E-Business Suite using Workflow Business Events. The Workflow Business Events have subscriptions that are enabled by default and if disabled will change the default behavior. The event subscriptions that an administrator may want to disable are:

- **Event:** oracle.apps.fnd.identity.add **Subscription:** assign_def_resp

  This event subscription will add the default responsibility "Preferences" when provisioning a new user from Oracle Directory Services to Oracle E-Business Suite.

- **Event:** oracle.apps.fnd.identity.add **Subscription:** hz_identity_add

  This event subscription will create TCA records when provisioning a new user from

Oracle Directory Services to Oracle E-Business Suite.

- **Event:** oracle.apps.fnd.identity.modify **Subscription:** hz_identity_modify

  This event subscription will modify TCA records when updates are made to a user in Oracle Directory Services.

Maintaining the Workflow Attribute Cache (Oracle E-Business Suite)

Data is synchronized between Oracle Directory Services and Oracle E-Business Suite using a Workflow attribute cache. The data resides in this table until manually removed by the system administrator. It is recommended that periodically the API WF_ENTITY_MGR.FLUSH_CACHE should be run to remove obsolete data. This API deletes cached records that match the specified entity information provided. When passing a specific entity_type (for example, 'USER'), the specific entity_key_value should also be passed. The special entity_type "*ALL*" will truncate the entire table.

Parameters for wf_entity_mgr.flush_cache

Name	Type	Direction	Default	Description
p_entity_type	varchar2	In	Null	Entity type to be deleted, for example 'USER'
p_entity_key_value	varchar2	In	Null	Entity value to be deleted, for example 'SCOTT'

Changing E-Business Suite Database Account Password

The APPS database account password is used to register a provisioning profile in Oracle Directory Services for a specific Oracle E-Business Suite instance. If the APPS database account password for that instance is changed using the AFPASSWD utility or FNDCPASS utility, the Oracle Directory Services provisioning profile must to be updated with the new information. This can be done by running the `manageProvProfiles` or `oidprovtool` command-line utility.

For more information about the AFPASSWD and FNDCPASS utilities, refer to the *Oracle E-Business Suite Maintenance Guide*.

manageProvProfiles Usage

The command syntax for this tool is:

```
manageProvProfiles operation=modify \
ldap_host=<LDAP_HOST> \
ldap_port=<LDAP_PORT> \
ldap_user_dn=<bindDN> \
application_dn="<LDAP distinguished name of application>" \
interface_connect_info=<Oracle E-Business Suite connect info of the
format, host:port:Sid:username:password>
```

> **Note:** For Oracle Internet Directory, `<bindDN>` is `cn=orcladmin`. For Oracle Unified Directory, `<bindDN>` is `cn=Directory Manager`.

For example:

```
manageProvProfiles operation=modify \
ldap_host=infra30qa  ldap_port=3060 \
ldap_user_dn="cn=orcladmin" \
application_dn="orclApplicationCommonName=ebizqa,cn=EBusiness,
cn=Products,cn=OracleContext,dc=com" \
interface_connect_info=ebiz30qa:1521:ebizqa:apps:password
```

Example output:

```
orclODIPProfileName=EA3EFF8640819A51F0301990304E5D0B_EA960F743D5D7552F03
01990304E34B3, cn=Provisioning Profiles, cn=Changelog Subscriber,
cn=Oracle Internet Directory
The Provisioning Profile for the Application has been modified.
```

For further details about the `manageProvProfiles` utility, see *Oracle Fusion Middleware Administering Oracle Unified Directory* or *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

oidprovtool Usage

Used for Oracle Internet Directory prior to 11.1.1.9, the command syntax for this tool is:

```
oidprovtool operation=modify \
ldap_host=<OID Server hostname> \
ldap_port=<OID Server Port> \
ldap_user_dn="cn=orcladmin" \
application_dn="<LDAP distinguished name of application>" \
interface_connect_info=<Oracle E-Business Suite connect info of the
format, host:port:Sid:username:password>
```

For example:

```
oidprovtool operation=modify \
ldap_host=infra30qa  ldap_port=3060 \
ldap_user_dn=cn="orcladmin" \
application_dn="orclApplicationCommonName=ebizqa,cn=EBusiness,
cn=Products,cn=OracleContext,dc=com" \
interface_connect_info=ebiz30qa:1521:ebizqa:apps:password
```

Example output:

```
orclODIPProfileName=EA3EFF8640819A51F0301990304E5D0B_EA960F743D5D7552F03
01990304E34B3, cn=Provisioning Profiles, cn=Changelog Subscriber,
cn=Oracle Internet Directory
The Provisioning Profile for the Application has been modified.
```

For further details about the `oidprovtool` utility, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

Manual Subscription Management With Provsubtool

Provsubtool Subscription Management Tool

Depending on how your Oracle E-Business Suite Single Sign-On profile options have been configured, it may be necessary to manage subscriptions for some of your users manually.

The Oracle Directory Services `provsubtool` command-line utility is used to manage application-specific subscription lists in Oracle Directory Services. The tool can be used by the application administrator or the Identity Management Realm administrator (such as orcladmin).

Use the provsubtool shipped under <DIP Oracle Home>/bin on the DIP side. Ensure that ORACLE_HOME is set to the DIP home and ORACLE_HOME/bin is in the PATH before running the command.

Specific uses of this tool are to:

- Add or remove users from application-specific subscription lists in bulk mode or batch mode.
- Add users to the application-specific subscription lists when Applications SSO Enable OID Identity Add Event profile value is 'Disabled'. This profile controls the automatic subscription for users created in Oracle Directory Services.
- List the memberships of a particular subscription list for an application.
- Read from a file of a list of simple user login names (nickname attribute values) or user DNs and add or remove them from the appropriate subscription list as specified.

Command Line Parameters

Parameter Name	Required or Optional	Default Value	Parameter Description
LDAP_HOST	Optional	Local host	LDAP server host
LDAP_PORT	Optional	389	LDAP Server port
APP_DN	Required	None	Application Identity DN, for example: `orclapplicationcommonname=Financials,cn=EBusiness,cn=Products,cn=OracleContext,<Identity Realm>`

Parameter Name	Required or Optional	Default Value	Parameter Description
APP_PWD	Required	None	Application DN password
REALM_DN	Required	None	DN of the identity Management Realm, for example: `dc=ganseycorp,dc=com`
LIST_NAME	Optional	ACCOUNTS	The Subscription List Name. By default, ACCOUNTS is created for Oracle E-Business Suite instances.
OPERATION	Required	None	ADD, REMOVE, LIST. The LIST option will list all the current members of the subscription list.
FILE_NAME	Optional	members.lst	File containing the user list either as simple names or DNs
FILE_TYPE	Optional	0	0 = Simple Names 1 = DNs
LOG_FILE	Optional	report.log	Output log file. The output from the command is written to a file specified by the parameter "LOG_FILE." If no filename is specified, the default of report.log is used.
DEBUG	Optional	0	Debugging On/Off (0 or 1)
MAX_ERRORS	Optional	1000	Abort operation after this number of errors have occurred. If the numbers of errors exceed the value specified by the "MAX_ERRORS" parameter (during a bulk operation when trying to add many users together in a batch), the command will fail.

Manually Adding and Removing Users

For an Oracle Financials E-Business Suite instance registered in Oracle Directory Services as: `orclapplicationcommonname=Financials,cn=EBusiness,cn=Products,cn=OracleContext,<Identity Realm>` for the ID realm: `dc=ganseycorp,dc=com`

To add a user whose nickname is "john.smith" to the default subscription list "ACCOUNTS," you would add the line "john.smith" (without the quotes) to an input

file, in this case with the default name of `members.lst`, and then run the command:

```
provsubtool ldap_host=LDAP_HOST ldap_port=LDAP_PORT \
app_dn="orclapplicationcommonname=Financials,cn=EBusiness,\
cn=Products,cn=OracleContext,dc=ganseycorp,dc=com" \
realm_dn="dc=ganseycorp,dc=com"
list_name=ACCOUNTS \
operation=ADD \
file_name=members.lst
file_type=0 \
app_pwd=tea4two
```

To remove a user, you would follow the same procedure, simply substituting the operation REMOVE for the operation ADD:

```
provsubtool ldap_host=LDAP_HOST ldap_port=LDAP_PORT \
app_dn="orclapplicationcommonname=Financials,cn=EBusiness,cn=Products,
cn=OracleContext,dc=ganseycorp,dc=com" \
realm_dn="dc=ganseycorp,dc=com"
list_name=ACCOUNTS \
operation=REMOVE \
file_name=members.lst
file_type=0 \
app_pwd=tea4two
```

Migrating Data Between Oracle E-Business Suite and Oracle Directory Services

The Oracle E-Business Suite Release 12.2 user migration utilities include:

- The *AppsUserExport* utility, which exports existing application accounts from Oracle E-Business Suite Release 12.2 into an intermediate LDIF file. This tool is a Java program that is invoked from the command line on an Oracle E-Business Suite application tier machine.

- The *LDAPUserImport* utility, which reads an LDIF file, creates new Oracle E-Business Suite application accounts as needed, and imports the data. This tool is invoked from the command line. `LDAPUserImport` is provided for bulk migration of existing Oracle Directory Services accounts into Oracle E-Business Suite Release 12.2.

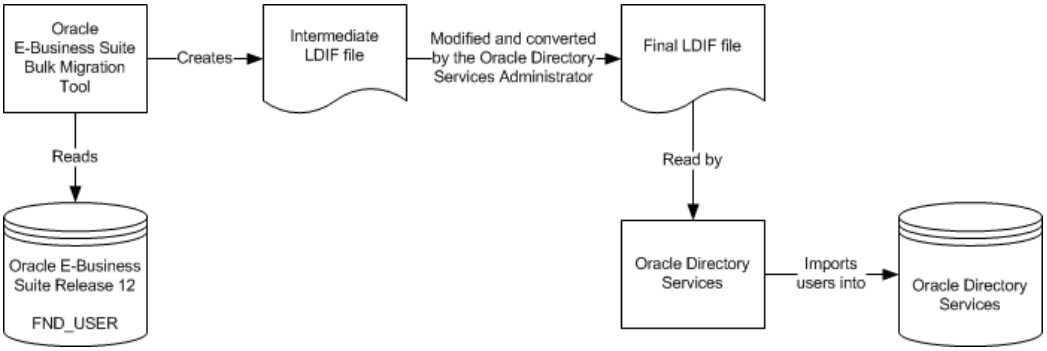
The following provides details of the migration process between Oracle E-Business Suite Release 12.2 and Oracle Directory Services, and the usage of these utilities.

Migrating Existing Application Accounts in Oracle E-Business Suite Release 12.2 to Oracle Directory Services

An Oracle E-Business Suite administrator can use the `AppsUserExport` utility to export a selected set of application accounts from the Oracle E-Business Suite native user directory (FND_USER) into an intermediate LDIF file. An Oracle Directory Services administrator then uses the Oracle Directory Services `ldifmigrator` tool to convert this intermediate LDIF file into a final LDIF file, based on Oracle Directory Services deployment choices. The Oracle Directory Services administrator then loads

the final LDIF file into Oracle Directory Services using either the `bulkload` or `import-ldif` utility. This process is depicted in the following diagram.

Process of Migrating Existing Application Accounts in Oracle E-Business Suite Release 12.2 to Oracle Directory Services



The migration process and intermediate LDIF format are explained further in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* and *Oracle Fusion Middleware Administering Oracle Unified Directory*. In addition, usage of the Oracle Internet Directory Data Migration Tool (`ldifmigrator`) is described in *Oracle Fusion Middleware Reference for Oracle Identity Management.*

> **Note:** Oracle E-Business Suite user passwords are stored as a non-reversable hash and cannot be recovered for export to Oracle Directory Services. After you implement password hashing, the AppsUserExport utility can no longer include the passwords when exporting Oracle E-Business Suite user information. For more information, see: "Using ADPASSWD to Migrate to a Password Hashing Scheme" in the *Oracle E-Business Suite Maintenance Guide*.

If you have an Identity Management solution configured for user password management, follow Option 1; otherwise, follow Option 2.

Option 1: Follow the instructions in this section if you use an Identity Management solution for your user password management (such as Oracle Identity Manager, Oracle Access Manager Password Management, Microsoft Active Directory, or another 3rd party LDAP for example).

1. Run the `AppsUserExport` utility without the `-g` option.
2. Follow the process to load the LDIF into Oracle Directory Services.
3. The Identity Management administrator should determine the best approach for their configuration to set the initial password of each user and communicate this to the users. This will be performed using the Identity Management solution used by your organization, which may be Oracle Identity Manager, Oracle Access Manager

Password Management, Microsoft Active Directory, or another third party LDAP.

Option 2: Follow the instructions in this section if you provision users between Oracle E-Business Suite and Oracle Directory Services and do not have an Identity Management solution configured for your user password management.

Before using this option, ensure that users will be synchronized from Oracle E-Business Suite to Oracle Directory Services by setting the Oracle Directory Services provisioning profile for deployment (provisioning type 1, 2, or 4) from Oracle E-Business Suite to Oracle Directory Services and enabling the Applications SSO LDAP Synchronization (APPS_SSO_LDAP_SYNC) profile option.

1. Run the `AppsUserExport` utility with the `-g` option.
2. Follow the process to create and load the LDIF into Oracle Directory Services. When loading the LDIF file, use the `bulkload` utility.
3. Expire these users' passwords using the `AFCPEXPIRE.sql` script.
4. Direct users to log in to Oracle E-Business Suite using the local login and change their passwords. Once a user's password is reset, the user should be able to log in using single sign-on.

The following focuses on application-specific tasks.

Task 1: Export Application Accounts into an Intermediate LDIF File

1. **Determine which accounts to migrate**

   Having determined which accounts to export, the application administrator can then specify whether an account is migrated by utilizing the following profiles:

   - **Applications SSO Login Types (APPS_SSO_LOCAL_LOGIN)** - An account will not be migrated if the user level profile value of the account is "LOCAL", that is, the account is a local account.
   - **Applications SSO LDAP Synchronization (APPS_SSO_LDAP_SYNC)** - An account will not be migrated if the user level profile value of the account is "N", that is, the account is marked to *not* synchronize with Oracle Directory Services.

   Oracle E-Business Suite ships a number of standard accounts, such as SYSADMIN and GUEST. These accounts should not be migrated. To enforce this, the `SYSADMIN` and `GUEST` accounts are pre-seeded with Applications SSO Login Types (APPS_SSO_LOCAL_LOGIN) set to "LOCAL" and Applications SSO LDAP Synchronization (APPS_SSO_LDAP_SYNC) set to "N".

   > **Important:** Accounts with user_id less than 10 can only be logged into locally, and **not** through single sign-on (you can check for

these with the query `select user_name from FND_USER where user_id < 10`).

2. **Use the AppsUserExport utility to extract user information**

   Use the `AppsUserExport` utility to extract application user information into an intermediate LDIF file. This utility is invoked from the command line.

   > **Note:** The list of attributes migrated to Oracle Directory Services from Oracle E-Business Suite is currently limited to those listed in Supported Attributes, page 5-93.

   To invoke the `AppsUserExport` utility, ensure your environment is set up correctly, and use the following syntax. Note that all parameters can if desired be entered on the same command line; they are shown here on different lines (using the UNIX '\' continuation character) for clarity.

```
java oracle.apps.fnd.oid.AppsUserExport \
[-v] \
[-oud] \
-dbc <dbcfile> \
-o <outputfile> \
-pwd <apps schema pwd> \
-g
[-l <logfile>]
```

   where:

   `[-v]` - Run in verbose mode

   `[-oud]` - Only required when directory server is Oracle Unified Directory

   `<dbcfile>` - Full path to the dbcfile

   `<outputfile>` - Intermediate LDIF file

   `<apps schema pwd>` - Apps schema password

   `-g` - Create and copy orclGuid users to Oracle Internet Directory, or entryUUID users to Oracle Unified Directory

   `<logfile>` - Log file (default is `<outputfile>.log`)

   Examples

   For Oracle Internet Directory:

```
java oracle.apps.fnd.oid.AppsUserExport -v -dbc \
$FND_SECURE/myebiz.dbc -o users.txt -pwd password -g -l users.log
```

   For Oracle Unified Directory (add option `-oud` on the command line):

```
java oracle.apps.fnd.oid.AppsUserExport -v -oud -dbc \
$FND_SECURE/myebiz.dbc -o users.txt -pwd password -g -l users.log
```

Warning: The resulting data file and log file may contain confidential information, such as the start and end dates for a user's account, and should therefore be secured appropriately.

Task 2: Convert the Intermediate LDIF File into a Final LDIF File

Before loading data into Oracle Directory Services by converting the intermediate LDIF file into the final LDIF file, the Oracle Directory Services administrator must ensure that:

- The extracted data file is copied from the Oracle E-Business Suite instance to Oracle Directory Services.
- If the provisioning profile has been set up for the Oracle E-Business Suite instance and the profile mode is either OUTBOUND or BOTH (i.e. you have enabled any provisioning events from Oracle Directory Services to Oracle E-Business Suite), the profile will need to be temporarily disabled during the migration process.
- The LDIF file contains the appropriate orclguid and entryUUID entry. For OID, the LDIF file must contain an orclguid entry and for OUD it must contain an entryUUID entry. If a mismatch is found, revisit the previous task (Task 1: Export Application Accounts into an Intermediate LDIF File) and ensure the correct option is specified when exporting user data using the `AppsUserExport` utility.

To convert the intermediate LDIF file to the final LDIF file format, an Oracle Directory Services administrator must instantiate certain variables in the intermediate LDIF file created by the `AppsUserExport` utility using the `ldifmigrator` tool. These variables are as follows:

- **s_UserContainerDN** - DN of the entry under which all users are added, for example `cn=users,dc=us,dc=oracle,dc=com`.
- **s_UserNicknameAttribute** - The nickname attribute used for user entries in the subscriber, such as uid.
- **s_UserNamingAttribute** - The RDN attribute used for user entries, by default: `cn` for Oracle Internet Directory or `uid` for Oracle Unified Directory

Examples

For Oracle Internet Directory

```
ldifmigrator "input_file=data.txt" \
"output_file=data.ldif" \
"s_UserContainerDN=cn=users,dc=us,dc=oracle,dc=com" \
"s_UserNicknameAttribute=uid" \
"s_UserNamingAttribute=cn"
```

For Oracle Unified Directory

```
ldifmigrator "input_file=data.txt" \
"output_file=data.ldif" \
"s_UserContainerDN=ou=people,dc=us,dc=oracle,dc=com" \
"s_UserNicknameAttribute=uid" \
"s_UserNamingAttribute=uid"
```

> **Important:** Note that the variable names above are case sensitive.

If you encounter problems running any of the Oracle Directory Services command-line tools such as `oidprovtool` or `ldapsearch`, refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* or *Oracle Fusion Middleware Administering Oracle Unified Directory* for more information.

Task 3: Load the Final LDIF file into Oracle Directory Services

Once the final LDIF file has been generated, the user data is ready to be uploaded into Oracle Directory Services. Import can be done in either online or offline mode. This section describes the basic commands required in offline mode.

> **Additional Information:** For further details, see *Oracle Fusion Middleware Administering Oracle Unified Directory* or *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

Before performing a bulk load, use the `manageProvProfiles` tool with operation=DISABLE to disable the profile before the migration is started (the `oidProvTool` tool CLI is still supported for backwards compatibility).

For example:

```
manageProvProfiles operation=disable \
ldap_host=testsys1.example.com \
ldap_port=3060 \
ldap_user_dn=cn=orcladmin \
application_dn="orclApplicationCommonName=beta,cn=EBusiness,cn=Products,
cn=OracleContext,dc=example,dc=com" \
profile_mode=BOTH
```

> **Important:** Do not add spaces after any of the commas in the `application_dn` parameter.

Loading the LDIF File into Oracle Internet Directory

1. Before using the `bulkload` utility to load the LDIF file, stop all Oracle Internet Directory processes running out of the Oracle Internet Directory Oracle home.

2. Load the LDIF file into Oracle Internet Directory, using the steps described in the following section, Preventing Collisions in Oracle Internet Directory, page 5-84.

Preventing Collisions in Oracle Internet Directory

The user namespaces contained in an LDIF file that is to be bulk loaded must be unique and non-overlapping. When bulk loading users into Oracle Directory Services, the potential for *collisions* (duplicate users) exists. Collisions can result when integrating multiple sources into a single Oracle Directory Services instance or by performing an import more than once for the same LDIF file. As collisions can lead to numerous problems, you should follow the steps below to ensure that they do not occur:

1. Run the `bulkload` utility with the `check` and `generate` options to verify that there are no duplicate users. For example:

   ```
   bulkload connect=<connect string> check=true generate=true
   file=<full path to LDIF file>
   ```

2. Check the log file for duplicate users.

3. If the log file indicates duplicate users, manually remove these users from the LDIF file.

4. Rerun Step 1 to verify all duplicates have been successfully removed.

5. Once all duplicates are removed, run the `bulkload` utility with the `-load` option to load the users. For example:

   ```
   bulkload connect=<connect string> load=true file=<full path to
   LDIF file>
   ```

   Additional Information: For further details of the `bulkload` utility, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

Instead of the `bulkload` utility, the `ldapadd` command can also be used for Oracle Internet Directory:

```
ldapadd -h <host> -p <port> -D "cn=orcladmin" -w <password> -f <full
path to ldif file>
```

Note that the `ldapadd` command cannot be used when the LDIF file contains users with no value for the userPassword attribute.

Warning: As some operating systems also include an `ldapadd` executable (which will not work with Oracle Directory Services), it is advisable to specify the full path of `$ORACLE_HOME/bin/ldapadd` to ensure the correct one is used.

Loading the LDIF File into Oracle Unified Directory

1. In offline mode, stop the directory server:

```
$ORACLE_INSTANCE/OUD/bin/stop-ds
```

2. Using the `import-ldif` utility, import the LDIF file into Oracle Unified Directory.

```
import-ldif -b ou=people,dc=example,dc=com -l <full path to LDIF
file> -n userRoot --append -R <path to rejected entries log file>
```

> **Caution:** The `--append` or `-a` option must be specified in order to append the entries, otherwise all existing entries in the backend directory server will be replaced.
>
> For further details on the `import-ldif` utility, see Appendix A of *Oracle Fusion Middleware Administering Oracle Unified Directory*.

Preventing Collisions in Oracle Unified Directory

The user namespaces contained in an LDIF file that is to be bulk loaded must be unique and non-overlapping. When bulk loading users into Oracle Directory Services, the potential for collisions (duplicate users) exists. Collisions can result when integrating multiple sources into a single Oracle Directory Service instance or by performing an import more than once for the same LDIF file. As collisions can lead to numerous problems, you should follow the steps below to ensure that they do not occur.

For Oracle Unified Directory, `import-ldif` can be used to avoid duplicate users. For example:

```
import-ldif -h localhost -port 4444 -D "cn=Directory Manager" -w
password -X -l /ldif-files/example.ldif --rejectFile rejected.ldif --
skipFile skipped.ldif
```

You can also use the `ldapmodify` command instead of `import-ldif` to avoid duplicate users:

```
ldapmodify -h <host> -p <port> -D "cn=Directory Manager" -w password -a
-f <full path to ldif file>
```

For further details on the `import-ldif` and `ldapmodify` utilities, see Appendix A of *Oracle Fusion Middleware Administering Oracle Unified Directory*.

Importing Multiple LDIF Files

It is possible to bulk load to import multiple LDIF files. The most common scenario is one in which multiple LDIF files are generated from different Oracle E-Business Suite instances. Consolidating user information from each Oracle E-Business Suite instance into a single Oracle Directory Services can reduce the administrative overhead of managing multiple user repositories.

The user namespaces from each Oracle E-Business Suite instance's LDIF file must be unique and non-overlapping. For example, if user name "John.Brown" exists in the LDIF file to be imported from Oracle E-Business Suite instance A, it must not exist in the LDIF file to be imported from Oracle E-Business Suite instance B. If these user names do not correspond to the same user, then the user name should be updated in Oracle E-Business Suite instance B. This will both distinguish between the two users and

eliminate the duplication. Otherwise, the user name must be removed from the LDIF file from instance B.

Once the LDIF file for Oracle E-Business Suite instance A has been bulk loaded into Oracle Directory Services, then the procedure should be done for the LDIF file for Oracle E-Business Suite instance B. By removing the duplicate users from the LDIF file, only the unique users from Oracle E-Business Suite instance B should bulk loaded into Oracle Directory Services. If a third Oracle E-Business Suite instance is to be bulk loaded, the same procedure should be carried out: after removing the duplicate users from the LDIF file, only the users unique to Oracle E-Business Suite instance C will be bulk loaded into Oracle Directory Services.

Final LDIF File Excerpts

The following sample is an excerpt from a final LDIF file for Oracle Internet Directory:

```
dn: cn=001, cn=Users,dc=example,dc=com
sn: 001
uid: 001
description: Testing OID sync
mail: 001@example.com
facsimileTelephoneNumber: 650-555-1111
orclActiveStartDate: 20181012000000z
orclIsEnabled: ENABLED
userPassword: {MD5}xxxxxxxxxxxxxxxxxxxxxx==
orclGuid: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
cn: 001
objectClass: inetOrgPerson
objectClass: orclUserV2
```

The following sample is an excerpt from a final LDIF file for Oracle Unified Directory:

```
dn: uid=001, ou=people,dc=example,dc=com
sn: 001
uid: 001
description: Testing OUD sync
mail: 001@example.com
facsimileTelephoneNumber: 650-555-1111
orclActiveStartDate: 20181012000000z
orclIsEnabled: ENABLED
userPassword: {MD5}xxxxxxxxxxxxxxxxxxxxxx==
entryUUID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
cn: 001
objectClass: inetOrgPerson
objectClass: orclUserV2
```

Password Restrictions and Bulk Loading

- Passwords stored in Oracle Directory Services are case-sensitive. Mixed-case passwords in Oracle E-Business Suite are migrated with the case preserved.

- The passwords in the LDIF file are encrypted using the MD5 hashing method. If errors occur while importing the LDIF file into Oracle Directory Services, check the hashing method used by Oracle Directory Services. If is not MD5, use ODM to reset the import hashing method to MD5 and try importing the LDIF file.

- When you export users from Oracle E-Business Suite and create an LDIF file, the

passwords are encrypted and so the bulk loader cannot verify if they follow Oracle Directory Services password policy. Therefore, the password policy cannot be enforced when such users are bulk-loaded into Oracle Directory Services.

Task 4: Update lastchangenumber and Restart the Oracle Directory Services Processes

1. Start all Oracle Directory Services processes.

2. Shutdown the Oracle Directory Integration Platform (DIP) by opening the Oracle Enterprise Manager Console for the DIP domain (`http://<AdminServerhost.domain>:<AdminServer_Port>/em`). In the navigation panel on the left, navigate to **Identity and Access** > **DIP(<version>)** > **DIP Server** > **Control** > **Shut Down**.

3. Update the `lastchangenumber` attribute of the profile. To do so, find the current last change number in Oracle Directory Services with the `ldapsearch` command:

   ```
   $ORACLE_HOME/bin/ldapsearch -h <host> -p <port> -D <bindDN> \
   -w <bindDN pwd> -s base -b "" "objectclass=*" \
   lastchangenumber
   ```

   Next, the `oidprovtool` command may be used to update the `lastchangenumber` attribute to the number `n` that was discovered in the last step. The `oidprovtool` command can be used with either Oracle Internet Directory or Oracle Unified Directory with the following syntax.

   ```
   oidprovtool operation=MODIFY \
   ldap_host=<ldap_host> \
   ldap_port=<ldap_port> \
   ldap_user_dn=<user to connect to LDAP> \
   ldap_user_password=<user password> \
   application_dn=<dn of the registered app for which the profile is
   modified> \
   orclLastAppliedChangeNumber=<n>
   ```

   For example:

   ```
   oidprovtool operation=MODIFY \
   ldap_host=testsys1.example.com \
   ldap_port=3060 \
   ldap_user_dn=cn=orcladmin \
   application_dn="orclApplicationCommonName=testsys1,cn=EBusiness,
   cn=Products,cn=OracleContext,dc=example,dc=com" \
   orclLastAppliedChangeNumber=100
   ```

   You can also use the `manageProvProfiles` command with the following syntax.

   > **Note:** For Oracle Internet Directory and Oracle Unified Directory 12c, `oidprovtool` is no longer used and therefore the `manageProvProfiles` command must be used instead.

```
manageProvProfiles operation=MODIFY \
ldap_host=<ldap_host> \
ldap_port=<ldap_port> \
ldap_user_dn=<bindDN> \
application_dn=<dn of the registered app for which the profile is
modified> \
lastchangenumber=<number>
```

For example:

```
manageProvProfiles operation=MODIFY \
ldap_host=testsys1.example.com \
ldap_port=3060 \
ldap_user_dn=cn=orcladmin \
application_dn="orclApplicationCommonName=testsys1,cn=EBusiness,
cn=Products,cn=OracleContext,dc=example,dc=com" \
lastchangenumber=100
```

> **Additional Information:** Reference the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform* for more information.

4. Use the `manageProvProfiles` tool with operation=ENABLE to enable the profile.

   For example:

```
manageProvProfiles operation=enable \
ldap_host=testsys1.example.com \
ldap_port=3060 \
ldap_user_dn=cn=orcladmin \
application_dn="orclApplicationCommonName=beta,cn=EBusiness,
cn=Products,cn=OracleContext,dc=example,dc=com" \
profile_mode=BOTH
```

5. Start up the DIP by opening the Oracle Enterprise Manager Console for the DIP domain (`http://<AdminServerhost.domain>:<AdminServer_Port>/em`). In the navigation panel on the left, navigate to **Identity and Access** > **DIP (<version>)** > **DIP Server** > **Control** > **Start Up**.

Task 5: Create Subscriptions for Bulk Loaded Users

The `bulkload` utility does *not* automatically subscribe users to the parent Oracle E-Business Suite instance. To create the subscriptions for your bulk loaded users, run the following SQL statement on your Oracle E-Business Suite database:

```
select user_name from FND_USER where
FND_profile.VALUE_SPECIFIC('APPS_SSO_LOCAL_LOGIN', user_id)<>'LOCAL' and
FND_profile.VALUE_SPECIFIC('APPS_SSO_LDAP_SYNC', user_id)='Y'
```

You can save the results of this query in a text file using your SQL client's capabilities. See Manual Subscription Management With Provsubtool, page 5-76 for details on how to run `provsubtool` to add these users to the subscription list.

Migrating Existing Accounts from Oracle Directory Services to Oracle E-Business Suite Release 12

The `LDAPUserImport` command-line utility takes an LDIF file generated from Oracle Directory Services, and inserts appropriate data into the Oracle E-Business Suite schema. It can be used for bulk migration of existing accounts from Oracle Directory Services to Oracle E-Business Suite. `LDAPUserImport` updates both FND and TCA schema.

> **Warning:** Importing user accounts and related information into Oracle E-Business Suite is a resource-intensive operation that may take a significant amount of time, as large amounts of business events and DML statements are issued in the process.

Task 1: Export Oracle Directory Services Users into the LDIF File

For Oracle Internet Directory

The Oracle Internet Directory `ldifwrite` command-line utility is used to create an LDIF file that can be loaded into the Oracle E-Business Suite schema by using the `LDAPUserImport` command-line utility.

Syntax and usage details for `ldifwrite` are described in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

General syntax of the command is as follows:

```
ldifwrite -c <db connect string> -b <base dn> -f <LDIF file>
```

For example:

```
ldifwrite -c asdb -b "cn=Users,dc=us,dc=example,dc=com" -f output.ldif
```

> **Note:** Do not modify the output file `output.ldif` in any way before proceeding with Task 2 below.

For Oracle Unified Directory

Oracle Unified Directory utilizes `ldapsearch` command-line utility to export users data. General syntax of the command is as follows:

```
$ORACLE_INSTANCE/OUD/bin/ldapsearch -h <host> -p <port> -D <bindDN> \
-w <bindDN pwd> -b "ou=people,dc=example,dc=com" -s sub
"(objectclass=orclUserV2)" \
dn orclguid cn sn mail userpassword description facsimiletelephonenumber
orclactivestartdate \
orclactiveenddate orclisenabled telephonenumber street postalcode
physicaldeliveryofficename \
ou st l displayname employeenumber employeetype givenname homephone
manager o uid c \
postaladdress title > export.ldif
```

For more information, see: *Oracle Fusion Middleware Administering Oracle Unified Directory*.

Task 2: Import LDAP Users into Oracle E-Business Suite Using the LDAPUserImport Utility

The `LDAPUserImport` utility is run from the command line using the following steps:

> **Note:** The list of attributes migrated to the Oracle E-Business Suite from Oracle Directory Services is limited to those described later in Supported Attributes, page 5-93.

1. Ensure the environment is set up properly.

2. Invoke the `LDAPUserImport` utility with the following syntax: Note that all parameters can be entered on the same command line; for clarity, they are shown on different lines here (using the UNIX '\' continuation character).

```
java oracle.apps.fnd.oid.LDAPUserImport \
[-v] \
-dbc <dbcfile> \
-f <ldiffile> \
-n <nicknameattribute> \
-b <size in integer> \
-d \
[-l <logfile>] \
[-tcaRecord <N or Y>] \
[-defresp <N or Y>]
```

where:

`[-v]` - Run in verbose mode.

`<dbcfile>` - Full path to the dbc file.

`<ldiffile>` - LDIF file.

`<nicknameattribute>` - Name of the attribute used as the nicknameattribute in OID.

`<logfile>` - Log file name. If not specified, the default is `LDAPUserImport.log`.

`-defresp` - Indicates whether to assign the default responsibility 'Preferences SSWA' to the uploaded users or not. Default is 'Y' (assign the responsibility).

For example:

```
java oracle.apps.fnd.oid.LDAPUserImport \
-v \
-dbc $FND_SECURE/myebiz.dbc \
-f users.ldif \
-n uid \
-l users.log
```

If the LDAP record already exists in the Oracle E-Business Suite instance, the following actions are taken:

1. The duplicate record is ignored.

2. The log file is updated with a reference to the duplicate record.

3. Processing continues to the next LDAP record.

Task 3: Create Subscriptions for Bulk Loaded Users

Refer to Manual Subscription Management With Provsubtool, page 5-76 for details on how to run the `provsubtool` utility in order to add the bulk loaded users to the subscription list.

Enabling and Disabling Users

Enabling and disabling events for users are raised and consumed differently in Oracle Directory Services and E-Business Suite.

Oracle E-Business Suite to Oracle Directory Services

New user accounts whose start date are in the future or end date in the past are currently not provisioned from Oracle E-Business Suite to Oracle Directory Services. Such pending user accounts have a corresponding place holder record created in the Oracle Directory Services: this record is either deleted or activated once the account request has been processed.

> **Important:** The IDENTITY_MODIFY event must be enabled in Oracle Directory Services to allow users to be enabled at the time of approval.

If an existing Oracle E-Business Suite user account is end-dated, the corresponding Oracle Directory Services account is not affected. This is because the Oracle Directory Services user may still require access to other partner applications. If no such access is needed, the relevant account will need to be disabled within Oracle Directory Services.

Oracle Directory Services to Oracle E-Business Suite

The status of an account in Oracle Directory Services is propagated to Oracle E-Business Suite as being either *enabled* or *disabled*. The application account start and end date are not updated, and users with local access to the applications should not be affected.

The default functionality can be customized by creating a Workflow subscription for the event oracle.apps.fnd.identity.modify. See Creating Custom Workflow Subscriptions, page 5-72 for details.

User accounts deleted from the Oracle Directory Services are end-dated in Oracle E-Business Suite, in order to maintain an audit trail.

Synchronizing Oracle HRMS with Oracle Directory Services

The Oracle HR Agent can be utilized to manage Oracle Human Resources employees in Oracle Directory Services, or to create E-Business Suite accounts automatically for new employees.

Definitions and Distinctions

An Oracle E-Business Suite *user* is someone who needs to be able to log into Oracle E-Business Suite. That user might need to file expense reports, view payslips, or file purchase requisitions. All Oracle E-Business Suite users have userids and records in the FND_USER repository, and have associated responsibilities that govern the functions and data that they can access.

An *employee* is someone whose information is managed by the Human Resources module in Oracle E-Business Suite. Oracle Human Resources tracks information such as employee numbers, manager hierarchies, and other personally identifiable information like birth dates.

Not all employees are users and vice versa. For example, a retailer might use Oracle E-Business Suite's Human Resources modules to manage employee information for their cashiers, but those cashiers may not be authorized to log into Oracle E-Business Suite at all.

From an organizational standpoint, this distinction enables the HR department to manage employees and the IT department to manage Oracle E-Business Suite accounts. Following on from the example above, consider a scenario where the cashiers are permitted to view their payslips by using the Self-Service Human Resources module. In such a case, the same person would be represented both in the Human Resources module and in the FND_USER repository. For Oracle E-Business Suite environments that are not integrated with Oracle Directory Services, user records need to be individually maintained in each location.

Creating Employee Entries in Oracle Directory Services

It is possible to use the Oracle Directory Services Human Resources connector to push employee information from Oracle HR to Oracle Directory Services:

Diagram of Flow Using Oracle Directory Services Human Resources to Push Employee Information

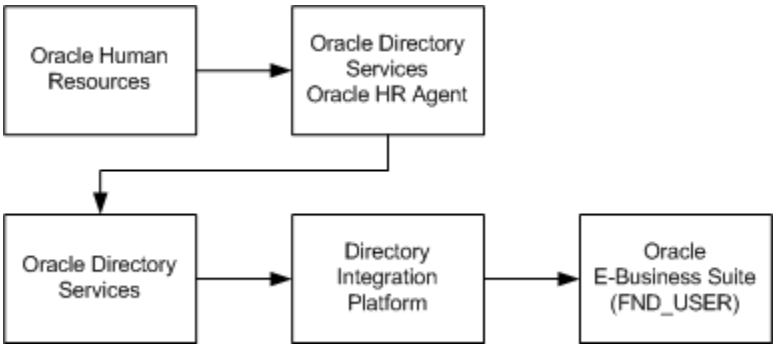
Note: Refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform* for more information.

A subset of employee data can be exported from Oracle Human Resources into Oracle Directory Services. The connector includes both a prepackaged integration profile, and an Oracle Human Resources agent that handles communication with Oracle Directory Services.

The Oracle Human Resources connector can be scheduled to run at any time, configuring it to extract incremental changes from the Oracle Human Resources system.

Administrators can set and modify mapping between column names in Oracle Human Resources and attributes in Oracle Directory Services. Since it is possible to provision users from Oracle Directory Services to Oracle E-Business Suite, the following flow can be configured:

Configuration Diagram to Provision Users from Oracle Directory Services to Oracle E-Business Suite



This architecture would support a business flow where a new employee is registered in E-Business Suite Human Resources by the HR department. That employee's information is then propagated using Oracle Directory Services to FND_USER, where an IT administrator grants the appropriate Oracle E-Business Suite responsibilities to the user account.

Important: The opposite direction is not supported. It is not possible to have an employee created in Oracle HR based upon a new user entry in Oracle Directory Services.

Supported Attributes

The following two tables list, respectively, the attributes that may be provisioned from Oracle Directory Services to Oracle E-Business Suite, and from Oracle E-Business Suite to Oracle Directory Services.

Note: This is a subset of the attributes listed in the provisioning templates.

Attributes Provisioned from Oracle Directory Services to Oracle E-Business Suite

Oracle Directory Services Attribute Name	FND_USER Column Name	TCA Table and Column Names
UID and [nickname]*	USER_NAME	
DESCRIPTION	DESCRIPTION	
FACSIMILETELEPHONENUMBER	FAX	
MAIL	EMAIL_ADDRESS	HZ_CONTACT_POINTS.EMAIL_ADDRESS (CONTACT_POINT_TYPE is 'EMAIL')
SN		HZ_PARTIES.PERSON_LAST_NAME
TELEPHONENUMBER		HZ_CONTACT_POINTS.RAW_PHONE_NUMBER (CONTACT_POINT_TYPE is 'PHONE' and CONTACT_POINT_PURPOSE is 'BUSINESS'
STREET		HZ_LOCATIONS.ADDRESS1
POSTALCODE		HZ_LOCATIONS.POSTAL_CODE
PHYSICALDELIVERYOFFICENAME		HZ_PARTY_SITES.MAILSTOP
ST		HZ_LOCATIONS.STATE
L		HZ_LOCATIONS.CITY

Oracle Directory Services Attribute Name	FND_USER Column Name	TCA Table and Column Names
GIVENNAME		HZ_PARTIES. PERSON_FIRST_NAME
HOMEPHONE		HZ_CONTACT_POINTS. PHONE_NUMBER (CONTACT_POINT_TYPE is 'PHONE' and CONTACT_POINT_PURPOSE is 'PERSONAL')
C		HZ_LOCATIONS.COUNTRY

* Refer to Recommended Nickname (Login Attribute) Setting, page 5-49 for more information.

Attributes Provisioned from Oracle E-Business Suite to Oracle Directory Services

FND_USER	Oracle Directory Services
USER_NAME	UID and [nickname]*
DESCRIPTION	DESCRIPTION
EMAIL_ADDRESS	MAIL
FAX	FACSIMILETELEPHONENUMBER
END_DATE	ORCLACTIVEENDDATE
START_DATE	ORCLACTIVESTARTDATE
START_DATE/END_DATE	ORCLISENABLED
ENCRYPTED_USER_PASSWORD	USERPASSWORD

* Refer to Recommended Nickname (Login Attribute) Setting, page 5-49 for more information. Also refer to Configuring Directory Integration Platform Provisioning Templates, page 5-66 for details of the provisioning process.

FND_SSO_UTIL Procedures

The FND_SSO_UTIL package contains procedures that provide capabilities to manage an SSO configuration.

enableLDAPIntegration

```
procedure enableLDAPIntegration
```

Used with the support of External/Internal Authentication first delivered in Release 12.2.6. This will set the preference indicating that the LDAP integration is enabled; and if the LDAP configuration is correct and complete, then provisioning will be enabled from Oracle E-Business Suite to LDAP.

disableLDAPIntegration

```
procedure disableLDAPIntegration
```

Used with the support of External/Internal Authentication delivered originally in Release 12.2.6. This will set the preference indicating that the LDAP integration is disabled and no provisioning will occur from Oracle E-Business Suite to LDAP.

deleteLDAPIntegration

```
procedure deleteLDAPIntegration
```

This API removes the value for checking if LDAP integration is enabled. Note that the LDAP registration itself is not affected.

setPasswordExternal

```
procedure setPasswordExternal(p_user_name_patt in varchar2,
p_upd_local_user in varchar2 default 'N')
```

This API will make the user's password externally managed. This API should be carefully used as the user's LDAP password must be accessible in OID/OUD.

To run this procedure for a user that is defined as a local user and is linked, set `p_upd_local_user` to 'Y'.

setUserLocalLoginProfile

```
procedure setUserLocalLoginProfile(p_user_name_patt in varchar2,
p_profile_value in varchar2)
```

This API will set the value of the profile APPS_SSO_LOCAL_LOGIN at the User level for the user or group of users to the value specified.

setUserLDAPSyncProfile

```
procedure setUserLDAPSyncProfile(p_user_name_patt in varchar2,
p_profile_value in varchar2)
```

This API will set the value of the profile APPS_SSO_LDAP_SYNC at the User level for the user or group of users to the value specified: 'Y', 'N', or null (the higher level will be used).

unlink_user

```
procedure unlink_user(p_user_name_patt in varchar2)
```

This API unlinks the FND user from the LDAP user.

link_batch

```
procedure link_batch(cuser in userCursor)
```

This API links the FND user or group of users with the LDAP user if the user is not currently linked.

References and Resources for Single Sign-On

This section lists some important resources for additional information that will be needed when planning and undertaking integration of Oracle E-Business Suite into a single sign-on environment. These should be used in conjunction with the references given in the chapter.

References

See the Oracle Fusion Middleware Documentation Library for a description of:

- Oracle Access Manager architecture and configuration
- Oracle WebLogic Server architecture and configuration
- The various single sign-on choices available for use with Oracle Fusion Middleware

Also see My Oracle Support Knowledge Document 1388152.1, *Overview of Single Sign-On Integration Options for Oracle E-Business Suite*, to find the recommended integration for your version of Oracle E-Business Suite and a reference to the detailed setup instructions and steps needed to perform this integration.

Glossary of Terms

CN

Common Name. May include a user name.

DN

Distinguished Name The DN uniquely identifies a user in the directory. It comprises all of the individual names of the parent entries, back to the root.

DIP

Directory Integration Platform, the infrastructure that keeps user information bidirectional synchronized between Oracle Directory Services, Oracle E-Business Suite Release 12, and third-party LDAP servers.

DIT

Directory information tree. A hierarchical tree-like structure consisting of the DNs of the entries.

GUID

Global Unique Identifier, a token used to identify a user's accounts in multiple systems during the single sign-on and enterprise level user management processes.

Identity Management Realm

A collection of identities, all of which are governed by the same administrative policies. In an enterprise, all employees having access to the intranet may belong to one realm, while all external users who access the public applications of the enterprise may belong to another realm. An identity management realm is represented in the directory by a specific entry with a special object class associated with it.

LDAP

The Lightweight Directory Access Protocol is a Internet-standard protocol and schema for user directories, and has gained widespread acceptance. LDAP was conceived as a standard, extensible directory access protocol for communication between suitably configured clients and servers. As a lightweight implementation of the International Standardization Organization (ISO) X.500 standard for directory services, LDAP requires a minimal amount of networking software on the client side, which makes it particularly attractive for Internet-based, thin client applications. Currently Oracle E-Business Suite Release 12 is certified to synchronize directly with Oracle Directory Services only. However, Oracle Directory Services can itself synchronize with one or more external, third-party user directories.

Oracle Access Manager

An Oracle Fusion Middleware component that can be integrated with Oracle E-Business Suite to provide a single sign-on solution.

Oracle E-Business Suite AccessGate

A Java Enterprise Edition application that can be used as part of a single sign-on solution for Oracle E-Business Suite. AccessGate is responsible for mapping a single sign-on user to an Oracle E-Business Suite user, and creating the Oracle E-Business Suite session for that user.

Oracle Directory Services

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.

Oracle Internet Directory

Oracle Internet Directory is a general-purpose directory service runs as an application on the Oracle database and enables retrieval of information about dispersed users and network resources. It combines LDAP Version 3 with the high performance, scalability, robustness, and availability of the Oracle database. It communicates with the database (which may be on the same or on a different operating system) via Oracle Net, Oracle's operating system-independent database connectivity solution. As noted above, Oracle E-Business Suite is certified to synchronize directly with Oracle Internet Directory only, but Oracle Internet Directory can itself synchronize with one or more external, third-party user directories. For more information, see *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

Oracle Unified Directory

Oracle Unified Directory is a comprehensive, next generation directory service that is designed to address large deployments, to provide high performance, to be highly extensive, and to be easy to deploy, manage, and monitor. It includes an LDAP directory server used for storing data, a proxy server where the server acts as an interface between the client and the directory server that contains the data, and a replication gateway between Oracle Unified Directory and Oracle Directory Server Enterprise Edition. For more information, see *Oracle Fusion Middleware Administering Oracle Unified Directory*.

Nickname Attribute

The attribute used to uniquely identify a user in the entire directory. The default value for this is uid. Oracle E-Business Suite uses this to resolve a simple user name to the complete distinguished name. The user nickname attribute cannot be multi-valued--that is, a given user cannot have multiple nicknames stored under the same attribute name.

Partner Application

An application that works within the Oracle single sign-on framework. It is designed (or has been modified) to delegate responsibility for user authentication to Oracle Access Manager. Oracle E-Business Suite Release 12.2 can be deployed as a partner application.

Provisioning

Refers to the process by which user information is synchronized between Oracle Directory Services and Oracle E-Business Suite. How provisioning is set up depends both on site requirements and the configuration in use.

Provisioning Profile

Metadata that controls details of the provisioning process between Oracle Directory Services and an Oracle E-Business Suite instance. A provisioning profile is required for each application that sends or receives provisioning events to or from Oracle Directory

Services.

Single Sign-On

Technology that allows a user to sign on once and gain access to multiple applications, instead of having to sign on to each application separately. In the context of Oracle E-Business Suite Release 12.2, refers to use of Oracle Access Manager to perform authentication, rather than the native FND_USER table.

Users

Individuals who have access to one or more software applications at a particular enterprise. Users are "global" entities, i.e. their existence and attributes exist outside the context of any particular software application.

User Directory

Software services that store the list of users and their attributes. Oracle E-Business Suite currently has its own proprietary user directory (the FND_USER table). There are also general purpose user directories that manage user information and expose it to integrated applications through a standard interface.

The Lightweight Directory Access Protocol (LDAP, see above for definition) is an example of a user directory.

Part 2

Secure Configuration

6

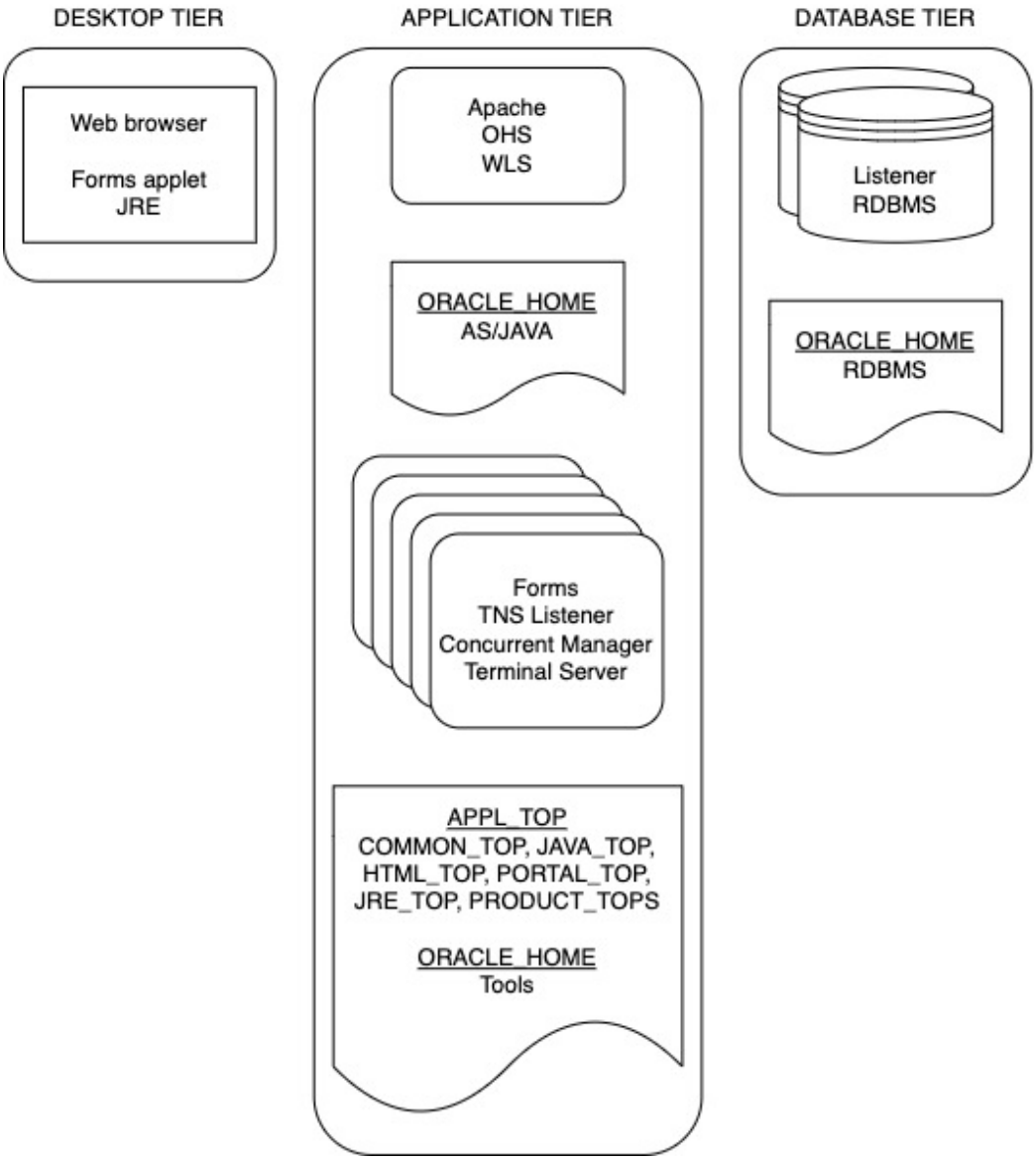
Overview of Secure Configuration

About Oracle E-Business Suite Secure Configuration

In today's environment, a properly secured computing infrastructure is critical. When securing the infrastructure, a balance must be struck between risk of exposure, cost of security, and value of the information protected. Each organization determines its own correct balance. To that end, we provide configuration guidance (practical advice) for securing Oracle's E-Business Suite.

The recommendations for securing your infrastructure cross the three-tier architecture that comprises an Oracle E-Business Suite installation. This architecture is made up of the desktop tier, which provides the user interface via an add-on component to a standard web browser; the application tier, which supports and manages the various Oracle E-Business Suite components, and is sometimes known as the middle tier; and the database tier, which supports and manages the Oracle database. The following diagram shows an overview of the Oracle E-Business Suite architecture.

Oracle E-Business Suite Architecture



The recommendations in these next chapters generally fall into one of five categories:

- **Hardening** covers hardening the file system, programs, products, and configuration.
- **Network** covers physical topology, firewalls, IP restrictions at web server and database listener.
- **Authentication** covers account management, password management, and other account related activities.

- **Authorization** covers restrictions to executables, data files, web pages, administrative tools, and so on.
- **Audit** covers configuration, on-going review, and purging.

We cover security for the database and listener, the application server, Oracle E-Business Suite, and individual desktops. We follow this with advice for hardening operating systems including a sample Linux hardening.

System-Wide Advice

Some advice applies to the entire Oracle E-Business Suite deployment and the infrastructure in which it operates.

Keeping Software Up-to-Date

One of the principles of good security practice is to keep all software versions and patches up-to-date. Throughout this document, we assume an Oracle E-Business Suite maintenance level of release 12.2 or later. The latest version of AutoConfig (TXK) configures a system following advice from this document. It also contains a patch set checker to assist with patch application. So for many good reasons, including good security practice, move to the latest version of AutoConfig and Patch Tools (AD).

Restricting Network Access to Critical Services

Oracle E-Business Suite secure configuration deployment guidelines include the following:

- **Use separate network subnets.**

  Deploy Oracle E-Business Suite application tier nodes in one subnet and the Oracle E-Business Suite database tier nodes in a separate subnet. Using separate subnets creates greater security for your Oracle E-Business Suite environment.

- **Use firewalls.**

  Keep both the Oracle E-Business Suite application tier and database tier behind a firewall. In addition, place a firewall between the application tier and database tier.

  The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and further restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls.

- **Use demilitarized zones (DMZ).**

  Follow the DMZ guidelines when exposing Oracle E-Business Suite to the internet. For more information, see My Oracle Support Knowledge <Document 1375670.1>, *Oracle E-Business Suite Release 12.2 Configuration in a DMZ*.

Following the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over ambitious granting of responsibilities, roles, grants, etc., especially early on in an organization's life cycle when people are few and work needs to be done quickly, often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Monitoring System Activity

System security stands on three legs: good security protocols, proper system configuration, and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this guide and regularly monitor audit records.

Keeping Up-to-Date on Latest Security Information

Oracle continually improves its software and documentation. Check this document regularly for revisions.

Oracle's Critical Patch Updates, security alerts, and bulletins are summarized at the following URL: https://www.oracle.com/security-alerts/.

Differences Between Oracle E-Business Suite Releases

This section provides an overview of the major differences in the technology stack and components between Oracle E-Business Suite Releases 11i, 12.0 or 12.1, and 12.2.

Updated Technology Stack

Oracle E-Business Suite Release 12 has updated the entire technology stack.

The table below summarizes the changes in Oracle E-Business Suite versions and highlights retired technology pieces.

Differences Between Oracle E-Business Suite Versions

Release 11i	Releases 12.0 and 12.1	Release 12.2
Database	None	None
9iR2 (9.2.0.x)	10g R2 (10.2.0.2.0)	11g R2 (11.2.0.3)
Application Tier	None	None

Release 11i	Releases 12.0 and 12.1	Release 12.2
IAS 1.0.2.2 + Developer 6i	Fusion Middleware	Fusion Middleware
OHS 1.0.2.2 (1.3.19 fork)	OHS 10.1.3 (1.3.34 fork)	OHS 11.1.1.6 (2.2.15 fork)
jserv	oc4j	WLS (10.3.6)
modplsql	-eliminated-	-eliminated-
Forms 6i	Forms 10.1.2.0.2	Forms 10.1.2.3
Reports 6i	Reports 10.1.2.0.2	Reports 10.1.2.3
Tools Oracle_home: 8.0.6	Tools Oracle_home: 10.1.2	Tools Oracle_home: 10.1.2
IAS Oracle_home: 8.1.7.4	Java Oracle_home: 10.1.3	OHS Oracle_home: 11.1.1.6 with: jRocket 1.6.0-29
JDBC 9 or 10	JDBC 10.2.0	JDBC 11.2
Desktop Tier	None	None
JRE for Forms applet: Oracle JInitiator	JRE for Forms applet: JRE 1.6 x._0x	JRE for Forms applet: JRE 1.6 or 1.7

Note that the versions listed are those that shipped with the initial, official release. Some of these versions may have gone out of support and been replaced with later point releases from the same overall release. For example, as of May 2019, the supported version for the OHS Oracle home is 11.1.1.9.

Modified Directory Structure

As of Oracle E-Business Suite Release 12, the way file systems are organized changed. From a security perspective, the most interesting point is the introduction of `INSTANCE_TOP` which is a new directory that contains instance specific configuration files and log files. This provides a cleaner separation of code directories and directories with instance specific and variable data. See *Oracle E-Business Suite Concepts Guide* for more details.

Key Updates in Oracle E-Business Suite Release 12.2

This section describes key updates found in Oracle E-Business Suite Release 12.2.

Online Patching

Oracle E-Business Suite Release 12.2 introduces a dual application tier file system to support online patching. One file system is the run file system and the other one is the patch file system. This way the system can keep running from the run file system while the patch file system is being patched.

Oracle E-Business Suite Release 12.2 utilizes the Edition-Based Redefinition feature of the Oracle Database to support online patching by using the "editioning view."

Online patching removes the traditional clear separation between runtime and patchtime windows.

Use of Native Fusion Middleware Tools

Another change in Oracle E-Business Suite Release 12.2 is that AutoConfig no longer manages the configuration of the Oracle Fusion Middleware components (OHS and WLS).

In Oracle E-Business Suite Release 12.2, many operations are performed using native Fusion Middleware (FMW) tools and procedures.

This means that following the initial install where configuration files are instantiated through the AutoConfig template files, subsequent modification for many files is performed interactively or scripted using FMW tools. Therefore, fixes and updates can no longer be provided as a patch to AutoConfig template files and instantiated by running AutoConfig.

Native Technology Stack Secure Configuration Guides

In Oracle E-Business Suite Release 12.2, the various technology stack components are so new at they have their own Secure Configuration Guide document. As part of "going native," you will have to become familiar with these product specific security guides as well.

7

Oracle TNS Listener Security

About Oracle TNS Listener Security

Oracle clients communicate with the database using the Transparent Network Substrate (TNS) protocol. When the listener receives a connection request (tcp port 1521, by default), it starts up a new database process and establishes a connection between the client and the database. This chapter contains security recommendations for the database TNS listener.

Hardening

Hardening Operating Environment

Follow the hardening instructions for Operating Environment Security, page 12-1.

Hardening External Procedure (EXTPROC) Services

The Oracle database uses the external procedure service to call external C programs. This extends the functionality of PL/SQL to routines that can be written in C to perform complex calculations, such as mathematical modeling or files system interactions. This functionality exploits the ability of the listener to issue operating system commands. The external procedures are supposed to issue the commands to the listener on a special IPC pipe named EXTPROC. The specification exists in the `listener.ora` parameter file as:

```
(ADDRESS_LIST = (ADDRESS = (PRTOCOL = IPC) (KEY = EXTPROC))
```

These external procedures operate by instructing the listener to issue these operating system commands on their behalf. Because the listener runs with the privilege of the operating system user, the only limits on external procedures are the limits on what that account can do.

The following Oracle E-Business Suite components use EXTPROC services:

1. Oracle Multimedia (formerly Oracle *inter*Media) cartridges
2. Oracle Email Center
3. Oracle Demand Planning Express implementation

To protect against some EXTPROC attack vectors:

1. Create two Oracle TNS listeners, one for the Oracle database and one for PL/SQL EXTPROC.
2. Remove EXTPROC specific entries from the Oracle Database listener configuration files.
3. Configure the Oracle EXTPROC listener with an IPC protocol address only.

   If TCP connectivity is required, configure a TCP protocol address, but use a port other than the one the Oracle listener for the database is using. Ensure that the Oracle listener created for PL/SQL EXTPROC runs as an unprivileged operating system user (e.g., "nobody" on UNIX). On Windows platforms, run the Oracle TNS listener process as an unprivileged user and not as the Windows LOCAL SYSTEM user. Give this user the operating system privilege to "Logon as a service."
4. If the Oracle listener for PL/SQL EXTPROC has been configured with a TCP address, do the following:
   1. Modify the EXTPROC specific entry in `$ORACLE_HOME/network/admin/tnsnames.ora` to reflect the correct port for the new Oracle listener.
   2. Enable Valid Node Checking and restrict access to those network clients requiring EXTPROC.
   3. Restrict access to the Oracle listener for PL/SQL EXTPROC only. Use a separate `$TNS_ADMIN/sqlnet.ora` file for this Oracle listener. Store this file in any directory other than the one in which the database `listener.ora` and `sqlnet.ora` files are located. Copy the `listener.ora` with the configuration of the Oracle listener for PL/SQL EXTPROC into this other directory as well. Before starting the Oracle listener for PL/SQL EXTPROC, set the TNS_ADMIN environment variable (or Windows Registry parameter) to specify the directory in which the new configuration files for PL/SQL EXTPROC are stored.
5. Ensure that the file permissions on separate `$TNS_ADMIN/listener.ora` are set to 600. Because it contains the password, only the owner should read the file.
6. Change the password to a strong password for any privileged database account or an ordinary user given administrative privileges in the database that has the ability

to add packages or libraries and access system privileges in the database (such as CREATE ANY LIBRARY). This step may not be applicable for default Oracle E-Business Suite implementations. This may be useful for customizations that involve addition of new schemas or customized PL/SQL code to be called as an external procedure service.

EXTPROC Listener Configuration

See below for the format of the dedicated EXTPROC listener. The parameters appear in `$TNS_ADMIN/listener.ora`. Replace the $ORACLE_SID with the name of the Oracle database instance (SID), $ORACLE_HOME with the value of ORACLE home directory for this listener, and $TNS_ADMIN with the directory location of the listener parameter files.

```
$ORACLE_SID_EXTPROC =
   (ADDRESS_LIST =
         (ADDRESS= (PROTOCOL= IPC)(KEY= EXTPROC$ORACLE_SID))
   )

SID_LIST_$ORACLE_SID_EXTPROC =
   (SID_LIST =
      (SID_DESC =
         (SID_NAME = PLSExtProc)
         (ORACLE_HOME = $ORACLE_HOME)
         (PROGRAM = extproc)
      )
   )

STARTUP_WAIT_TIME_$ORACLE_SID_EXTPROC = 0
CONNECT_TIMEOUT_$ORACLE_SID_EXTPROC = 10
TRACE_LEVEL_$ORACLE_SID_EXTPROC = OFF

LOG_DIRECTORY_$ORACLE_SID_EXTPROC = $TNS_ADMIN
LOG_FILE_$ORACLE_SID_EXTPROC = $ORACLE_SID_EXTPROC
TRACE_DIRECTORY_$ORACLE_SID_EXTPROC = $TNS_ADMIN
TRACE_FILE_$ORACLE_SID_EXTPROC = $ORACLE_SID_EXTPROC
```

The configuration below should appear in `$TNS_ADMIN/tnsnames.ora`. Replace $ORACLE_SID with the name of the Oracle database instance (SID).

```
extproc_connection_data =
         (DESCRIPTION=
            (ADDRESS_LIST =
               (ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC$ORACLE_SID))
            )
            (CONNECT_DATA=
               (SID=PLSExtProc)
               (PRESENTATION = RO)
            ) )
```

Example: EXTPROC Listener Configured Separately

This example shows how to configure EXTPROC listener services. In it, the LISTENER NAME is VSEC_EXTPROC and ORACLE_SID is VSEC.

```
VSEC_EXTPROC =
   (ADDRESS_LIST =
         (ADDRESS= (PROTOCOL= IPC)(KEY= EXTPROCVSEC))
   )

SID_LIST_VSEC_EXTPROC =
   (SID_LIST =
      (SID_DESC =
         (SID_NAME = PLSExtProc)
         (ORACLE_HOME = /u01/oracle/vsecdb/10.2.0.5)
         (PROGRAM = extproc)
      )
   )

STARTUP_WAIT_TIME_VSEC_EXTPROC = 0
CONNECT_TIMEOUT_VSEC_EXTPROC = 10
TRACE_LEVEL_VSEC_EXTPROC = OFF

LOG_DIRECTORY_VSEC_EXTPROC = /u01/oracle/vsecdb/10.2.0.5/network/admin
LOG_FILE_VSEC_EXTPROC = VSEC_EXTPROC
TRACE_DIRECTORY_VSEC_EXTPROC = /u01/oracle/vsecdb/10.2.0.5/network/admin
TRACE_FILE_VSEC_EXTPROC = VSEC_EXTPROC
```

Example: The tnsnames.ora Parameter That Corresponds to EXTPROC Listener

```
extproc_connection_data =
         (DESCRIPTION=
            (ADDRESS_LIST =
               (ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROCVSEC))
            )
            (CONNECT_DATA=
               (SID=PLSExtProc)
               (PRESENTATION = RO)
            ) )
```

EXTPROC Testing Procedure

This section explains a procedure to test if EXTPROC is enabled. The EXTPROC listener must be configured and working for the Oracle Multimedia option to run. Perform the following to test whether or not Oracle Multimedia is working:

1. Create a user to work with Oracle Multimedia text:

   ```
   create user textuser identified by <password>
   default tablespace users temporary tablespace temp;
   ```

2. Grant 'ctxapp' role to textuser:

   ```
   grant connect, resource, ctxapp to textuser;
   ```

3. Connect as textuser and create required test objects:

```
connect textuser/<password>

drop table quick;

create table quick (
   quick_id     number     constraint quick_pk primary key,
   text         varchar2(80)  0;

insert into quick ( quick_id, text ) values ( 1, 'The cat sat on the
mat' );
insert into quick ( quick_id, text ) values ( 2, 'The quick brown
fox jumps over
the lazy dog' );
insert into quick ( quick_id, text ) values ( 3, 'The dog barked
like a dog' );
commit;

create index quick_text on quick ( text ) indextype is ctxsys.
context;

col text format a45
col s format 999
select text, score(42) s from quick
   where contains ( text, 'dog', 42 ) >= 0
   order by s desc;
```

If the above query works without any error, the Oracle Multimedia option is enabled and the EXTPROC listener is properly configured.

Cleanup the test user (`textuser`) created during this test.

Network

Adding IP Restrictions / Enable Valid Node Checking

Valid Node Checking allows or denies access from specified IP addresses to Oracle services. Oracle recommends using an allowlist of IP addresses that are authorized to make a TCP connection to the database listener. To enable Valid Node Checking, set the following parameters in `$TNS_ADMIN/sqlnet.ora`:

```
tcp.validnode_checking = YES
tcp.invited_nodes = ( x.x.x.x, hostname.domain, ... )
```

The first parameter turns on Valid Node Checking. The next parameter specify the IP addresses or host names that are permitted to make network connections to the database. Replace x.x.x.x with the application tiers' IP addresses. Application tier components include web servers, forms servers, concurrent managers, terminal servers, central administrator machines, and any remote monitoring tool that uses SQL*Net.

> **Note:** The use of SQLNet desktop clients such as sqlplus, sqldeveloper, toad, or ADI from a windows desktop is not recommended on production databases. If implemented, the desktop cannot use DHCP (unless the DHCP server is configured with address reservation). Oracle recommends that only trusted servers be allowed to make direct

database connections.

AutoConfig supports automated configuration of this setting. If the profile option "SQLNet Access" (FND_SQLNET_ACCESS) is set to "ALLOW_RESTRICTED" at the site level when AutoConfig is run on the database server, AutoConfig will add IP restrictions to `sqlnet.ora`. The list of host will be all those from the FND_NODES table that are registered as an Oracle E-Business Suite node.

For more information, refer to the "Technical Configuration" chapter of the *Oracle E-Business Suite Setup Guide*, Release 12.2.

The easiest way to verify this is to implement a manual check from a node not in the allowlist. You should not be able to connect (by using Ncat, for example) to the database listener port. When connecting through an untrusted node, it should look like this:

```
# nc -v db.example.com 1521
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Connected to X.X.X.X:1521.

Ncat: Broken pipe.
```

The listener log will show this for a connection attempt from a client that is not "invited".

```
  ...
  <txt> Incoming connection from Y.Y.Y.Y rejected
  ...
  <txt> TNS-12546: TNS:permission denied
   TNS-12560: TNS:protocol adapter error
   TNS-00516: Permission denied
```

Specifying Connection Timeout

In `$TNS_ADMIN/listener.ora` , set the following parameter:

```
CONNECT_TIMEOUT_$ORACLE_SID = 10
```

For example:

```
CONNECT_TIMEOUT_PRD12 = 10
```

Where PRD12 is the value of the ORACLE_SID in this example.

Use the parameter CONNECT_TIMEOUT to specify the amounts of time, in seconds, for the Oracle listener to wait for the connection from a client to complete.

Enabling Encryption of Network Traffic

This section describes configuration options and recommendations for enabling encryption of database network traffic.

The following table is a summary of the three available configurations for encrypting traffic to the Oracle E-Business Suite database, which are described in more detail in the sections to follow.

Configuration Options for Encrypting Network Traffic to the Oracle E-Business Suite Database

Configuration Option	Database	Oracle E-Business Suite Application Tier Connections	Other Client Connections
Configuration 1: Enable Native Network Encryption on the Database Listener and Use TCP for All Client Connections	TCP with Native Network Encryption (NNE)	TCP	TCP
Configuration 2: Enable Native Network Encryption on the Database Listener and Enable TCPS for Non-Oracle E-Business Suite Application Tier Client Connections	TCP with NNE	TCP	TCPS
Configuration 3: Enable TCPS for All Client Connections	TCPS	TCPS using Oracle Connection Manager (CMAN)	TCPS

Configuration 1: Enable Native Network Encryption on the Database Listener and Use TCP for All Client Connections

In this configuration, native network encryption (NNE) is enabled on the database listener and a TCP connection is used for both Oracle E-Business Suite and non-Oracle E-Business Suite clients.

For most environments, NNE in conjunction with following guidance for Oracle E-Business Suite secure configuration deployment is sufficient for securing connections to your database. Oracle E-Business Suite secure configuration deployment provides additional protection for your Oracle E-Business Suite application and database tiers and includes the use of subnets, firewalls, and DMZs.

To set up Configuration 1, perform the following steps:

1. Deploy your Oracle E-Business Suite environment per the recommendations outlined in Restricting Network Access to Critical Services, page 6-3 in "Overview of Secure Configuration."

2. Enable NNE for the database using the following steps:

   1. Add the following lines to the `$TNS_ADMIN/sqlnet_ifile.ora` in your database Oracle home:

      ```
      SQLNET.ENCRYPTION_SERVER=REQUIRED
      SQLNET.ENCRYPTION_TYPES_SERVER=(AES128,AES192,AES256)
      SQLNET.CRYPTO_CHECKSUM_SERVER=REQUIRED
      SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER=(SHA256,SHA1)
      SQLNET.CRYPTO_SEED=<SEED>
      SQLNET.IGNORE_ANO_ENCRYPTION_FOR_TCPS=TRUE
      ```

      The value for SQLNET.CRYPTO_SEED for your deployment should be a random string of up to 70 characters.

   2. If you have applied the July 2021 Database CPU or later, also add the following to the `$TNS_ADMIN/sqlnet_ifile.ora` in your database Oracle home :

      ```
      SQLNET.ALLOW_WEAK_CRYPTO_CLIENTS=TRUE
      ```

   3. Restart the database listener.

Configuration 2: Enable Native Network Encryption on the Database Listener and Enable TCPS for Non-Oracle E-Business Suite Application Tier Client Connections

If you determine that encryption of database client connections other than the Oracle E-Business Suite application tier node database connections is a requirement for your environment, in addition to NNE you may enable TCPS for these client connections to the Oracle E-Business Suite database.

To set up Configuration 2, perform the following steps:

1. Enable NNE for the database using the instructions in step 2 of Configuration 1, page 7-8.

2. Enable TCPS for non-Oracle E-Business Suite application tier client connections. For more information, see My Oracle Support Knowledge Document 2867473.1, *Enable TCPS (TLS1.2) for Clients Outside the Oracle E-Business Suite Application Tier*.

Configuration 3: Enable TCPS for All Client Connections

If you determine that encryption of all database client connections including Oracle E-Business Suite application tier connections is a requirement for your environment, you may enable TCPS for all database client connections to the Oracle E-Business Suite database. Refer to My Oracle Support Knowledge Document 2787151.1, *Enable TCPS (TLSv1.2) for SQL*Net Traffic in Oracle E-Business Suite Release 12.2*.

Authorization

Enabling Admin Restrictions

You should configure the database listener with ADMIN_RESTRICTIONS set to ON. When ADMIN_RESTRICTIONS is ON, all the set commands in `lsnrctl` are disabled and the only way to change the configuration is to edit the `listener.ora` file.

In `$TNS_ADMIN/listener.ora`, set the following parameter:

```
ADMIN_RESTRICTIONS_<listener>=ON
```

For example:

```
ADMIN_RESTRICTIONS_VIS12=ON
```

where `VIS12` is the name of the listener (equal to `ORACLE_SID` in Oracle E-Business Suite)

AutoConfig can set this if you set the AutoConfig variable s_admin_restrictions to ON and run AutoConfig on the database server.

Audit

Enabling TNS Listener Logging

To enable logging, in `$TNS_ADMIN/listener.ora` set the following parameters:

```
LOG_STATUS = ON
LOG_DIRECTORY_$ORACLE_SID = $TNS_ADMIN
LOG_FILE_$ORACLE_SID = $ORACLE_SID
```

For example:

```
LOG_STATUS = ON
LOG_DIRECTORY_VIS12 = /u/db/tech_st/10.2.0/network/admin/VIS12_dbs01
LOG_FILE_VIS12 = VIS12
```

Where `VIS21` is the `LISTENER_NAME`.

This is done by default in Release 12.

Notice that newer database versions use the richer ADR log settings. This silently overrides/ignores the older LOG settings. See Oracle Database documentation for more details.

8

Oracle Database Security

About Oracle Database Security

Note that depending on the version you are running and how you arrived at that version, some of these settings may have been set by default. All you have to do in that case is verify that the settings are as described here. This chapter contains security recommendations for the database.

Hardening

Hardening Operating Environment

Follow the hardening instructions for Operating Environment Security, page 12-1.

Disabling XDB

To support XDB, the TNS listener process listens on two additional TCP ports: 2100 for FTP access and 8080 for http access. Oracle E-Business Suite does not require these services; they should be disabled.

To disable XDB, remove or comment out the line in `init.ora` that reads:

```
*.dispatchers='(PROTOCOL=TCP) (SERVICE=sidXDB)'
```

Review Database Links

Review database links in both production and development environments and drop those that are not required in your environment.

Optional Secure Configurations

Security policy must balance risk of attack, cost of defense and value of data protected.

This section contains recommendations that improve security, but may not be appropriate for every deployment.

Transparent Data Encryption (TDE)

Transparent data encryption (TDE) protects the data at rest by encrypting the data stored in the database data files. Oracle E-Business Suite Release 12.2 is certified with Column Encryption and Tablespace Encryption. See the following My Oracle Support knowledge documents for details:

- Document 1585296.1 - *Using TDE Tablespace Encryption with Oracle E-Business Suite Release 12.2*
- Document 1585696.1 - *Using TDE Column Encryption with Oracle E-Business Suite Release 12.2*

Column level TDE has a number of restrictions related to data types and indexed columns. Tablespace TDE does not have these restrictions and does not increase the storage requirement.

Authentication

Applications found on the application tier log on to the database through application schemas rather than end-user accounts. Some individuals (IT Administrators) may require direct access to the application database using their own schema.

Removing Operating System Trusted Remote Logon

This setting prevents the database from using an insecure logon protocol. Make sure `init.ora` contains:

```
REMOTE_OS_AUTHENT=FALSE
```

Changing Default Installation Passwords

Following an installation, the application database instance contains default, open schemas with default passwords. These accounts and corresponding passwords are well-known, and they should be changed, especially for a database to be used in a production environment. Default schemas come from different sources:

1. Default database administration schemas
2. Schemas belonging to optional database features neither used nor patched by Oracle E-Business Suite
3. Schemas belonging to optional database features used but not patched by Oracle E-Business Suite

4. Schemas belonging to optional database features used and patched by Oracle E-Business Suite

5. Schemas common to all Oracle E-Business Suite products

6. Schemas associated with specific Oracle E-Business Suite products

> **Note:** Starting in Oracle E-Business Suite Release 12.1.2, a new command-line utility named AFPASSWD is available to replace FNDCPASS. The new utility does not require passwords on the command line. Just like FNDCPASS, AFPASSWD is installed on the application tier and requires the libraries from the Tools Oracle home.

For the schemas in categories 1, 2, and 3, use standard database commands to change a password:

```
SQL> alter user <SCHEMA> identified by <NEW_PASSWORD>;
```

For the schemas in categories 4, 5, and 6 where Oracle E-Business Suite is "managing" the passwords, use the application password change tool AFPASSWD (or FNDCPASS):

```
$ AFPASSWD -c apps -o <SCHEMA>
```

You will be prompted for the APPS password and the new password (twice).

To save time, category six (6) schema passwords may be changed en masse using AFPASSWD. This is really handy as there are more than 200 schema passwords. AFPASSWD takes the `-a` option which will change all category 6 passwords to the new password (this works the same as the ALLORACLE mode in FNDCPASS).

```
$ AFPASSWD -c apps -a
```

You will be prompted for the APPS password and the new password (twice).

To determine which schemas are managed by Oracle E-Business Suite (categories 4, 5, and 6), run the AD `adutconf.sql` script.

Appendix B: Database Schemas Found in Oracle E-Business Suite, page B-1 contains a list of the schemas by category, instructions, and notes for managing schema passwords.

AFPASSWD only prompts for the passwords required for the current operation, allowing separation of duties between application administrators and database administrators. This also improves interoperability with Oracle Database Vault.

AFPASSWD is documented in the *Oracle E-Business Suite Maintenance Guide*.

Implementing Two Profiles for Password Management

The database provides parameters to enforce password management policies. However, some of the database password policy parameters could lock out the Oracle E-Business Suite. Because of this, we make specific recommendations for or against using certain

management features depending upon schema type.

Database "profiles" contain limits on database resources and password policies. Create two database profiles: one for application schemas on the application tier ("managed schemas") and one for human beings. Assign application schemas on the application tier to the first profile and all accounts used by individual database administrators to the second profile.

Application and Administrator Profile Password Parameters

Password Parameters	Application Profile	Administrator Profile
`FAILED_LOGIN_ATTEMPTS`	`UNLIMITED`	5
`PASSWORD_LIFE_TIME`	`UNLIMITED`	90
`PASSWORD_REUSE_TIME`	180	180
`PASSWORD_REUSE_MAX`	`UNLIMITED`	`UNLIMITED`
`PASSWORD_LOCK_TIME`	`UNLIMITED`	7
`PASSWORD_GRACE_TIME`	`UNLIMITED`	14
`PASSWORD_VERIFY_FUNCTION`	*Recommended*	*Recommended*

For more information on profiles, see CREATE PROFILE in the Oracle SQL reference documentation.

See Appendix B: Database Schemas Found in Oracle E-Business Suite, page B-1 for a list of all default database users and whether it is a managed schema.

Authorization

Restricting Access to SQL Trace Files

The `init.ora` parameter `_TRACE_FILES_PUBLIC` grants file system read access to anyone who has activated SQL tracing. Set this to its default value of *False*.

```
_TRACE_FILES_PUBLIC=FALSE
```

Removing Operating System Trusted Remote Roles

Set the `init.ora` parameter `REMOTE_OS_ROLES` to *False* to prevent insecure remote

roles.

```
REMOTE_OS_ROLES=FALSE
```

Limiting File System Access Within PL/SQL

The parameter `UTL_FILE_DIR` limits file system access for all database accounts using the PL/SQL API `UTL_FILE`. Oracle E-Business Suite requires the `UTL_FILE_DIR` database initialization parameter to be set when you are using Oracle Database 11g Release 2 or Oracle Database 12c Release 1. See My Oracle Support Knowledge Document 2525754.1, *Using UTL_FILE_DIR or Database Directories for PL/SQL File I/O in Oracle E-Business Suite Releases 12.1 and 12.2*.

```
UTL_FILE_DIR=<dir1>,<dir2>,<dir3>...
```

Avoid:

```
UTL_FILE_DIR=*
```

Limiting Dictionary Access

Set `O7_DICTIONARY_ACCESSIBILITY` to *False* to prevent users with the 'Select ANY' privilege from reading data dictionary tables. False is the default for the 10g database.

```
O7_DICTIONARY_ACCESSIBILITY = FALSE
```

Revoking Unnecessary Grants Given to APPLSYSPUB

The following table lists the privileges that should be granted to the APPLSYSPUB schema. These can be set by `<FND_TOP>/patch/115/sql/afpub.sql` or fixed by `<FND_TOP>/patch/115/sql/afpubfix.sql`.

Privileges to be Granted to the APPLSYSPUB Schema
EXECUTE ON FND_DISCONNECTED
EXECUTE ON FND_MESSAGE
EXECUTE ON FND_PUB_MESSAGE
EXECUTE ON FND_SECURITY_PKG
EXECUTE ON FND_WEBFILEPUB
INSERT ON FND_SESSIONS
INSERT ON FND_UNSUCCESSFUL_LOGINS

Privileges to be Granted to the APPLSYSPUB Schema
SELECT ON FND_APPLICATION
SELECT ON FND_APPLICATION_TL
SELECT ON FND_APPLICATION_VL
SELECT ON FND_LANGUAGES_TL
SELECT ON FND_LANGUAGES_VL
SELECT ON FND_LOOKUPS
SELECT ON FND_PRODUCT_GROUPS
SELECT ON FND_PRODUCT_INSTALLATIONS
SELECT ON FND_NEW_MESSAGES

The following table lists privileges required for online patching in Oracle E-Business Suite Release 12.2:

Privileges Required for Oracle E-Business Suite Release 12.2 Online Patching
INSERT ON FND_SESSIONS#
INSERT ON FND_UNSUCCESSFUL_LOGINS#
SELECT ON FND_APPLICATION#
SELECT ON FND_APPLICATION_TL#
SELECT ON FND_LANGUAGES_TL#
SELECT ON FND_PRODUCT_GROUPS#
SELECT ON FND_PRODUCT_INSTALLATIONS#
SELECT ON FND_NEW_MESSAGES#

To check permissions, log in as APPS and issue the following query:

```
SELECT * FROM dba_tab_privs WHERE grantee ='APPLSYSPUB';
```

9

Oracle Application Tier Security

About Oracle Application Tier Security

This section contains security recommendations for the Oracle E-Business Suite application tier.

Hardening

Hardening Operating Environment

Follow the hardening instructions for Operating Environment Security, page 12-1.

Configuring Allowed Resources

As of Oracle E-Business Suite Release 12.2.6 with Patch 24737426:R12.FND.C, the feature formerly known as Allowed JSPs has been enhanced and is now called Allowed Resources. This feature is an allowlist of resources that are authorized to be called by your system. The purpose of this configuration option is to reduce the attack surface of the deployed Oracle E-Business Suite instance. When Oracle E-Business Suite is installed, it installs resources for all modules in Oracle E-Business Suite. As you probably do not run every existing Oracle E-Business Suite module, you should configure your system to only allow the resources actually used in your deployment.

For more information on this feature, see Allowed Resources, page 4-82. You can also find detailed instructions on how to disable and enable products at the family level in Management by Product Hierarchy, page 4-88.

Configuring Allowed Redirects

The Allowed Redirects security feature in Oracle E-Business Suite, introduced in Release 12.2.4, provides defense in-depth protection against phishing redirect attacks by enabling the configuration of allowed redirects to avoid unnecessary exposure.

Similar to the Allowed Resources feature, Allowed Redirects restrict redirects by utilizing an allowlist mechanism, defining hosts with allowed access to a resource and denying access to those that are not in the allowed listing.

For more information, see Allowed Redirects, page 4-101.

Authorization

Within Oracle Application Server, a number of web pages provide administrative and diagnostics functionality. These pages offer information about various services, the server's state, and its configuration. While useful for debugging, these pages must be restricted or disabled in a production system.

Protecting Administrative Pages

The Apache configuration file `trusted.conf` is used to limit access to "administrative pages."

Oracle E-Business Suite ships with a number of pages that are useful when you need them, but the general user population should not have access to them. The pages include functionality used for monitoring and diagnostics, so access should be restricted to a number of fixed IP addresses such as the application tiers themselves and the administrator's fixed IP workstation.

The `trusted.conf` file contains directives such as the following:

```
<Location of "uri-to-protect">
  Order deny, allow
  Deny from all
  Allow from localhost <list of TRUSTED IPs>
</Location>
```

The `uri-to-protect` is the path to the page that will be restricted. The `<list of TRUSTED IPs>` will be replaced with the value of the AutoConfig variable s_admin_ui_access_nodes which you should set to the list of host machines from which administrators connect.

To allow the administrators access to the restricted pages, enter the fixed IP address (or resolvable host name) of their workstation in the AutoConfig variable s_admin_ui_access_nodes and run AutoConfig.

Considerations for Reverse Proxies and Load Balancers

The previously described restrictions work well when OHS is your web entry point.

If you put a reverse proxy or a load balancer in front of OHS, OHS will only see the IP address of the proxy or load balancer. To access restricted pages only from trusted hosts, you have two options:

1. Make the proxy pass the IP address of the client to OHS and make OHS read it - then `trusted.conf` will work as-is.

2. Implement equivalent rules in your proxy/load balancer and then either list the load balancer's IP address as trusted in `trusted.conf`

For more information about using reverse proxies or load balancers with Oracle E-Business Suite, see My Oracle Support Knowledge Document 1375686.1, *Using Load-Balancers with Oracle E-Business Suite Release 12.2*.

Considerations for Adding Pages to trusted.conf

If you find other pages that you wish to place similar restrictions on, you can add them to a customized version of the AutoConfig template for `trusted.conf` or to `custom.conf`. The `custom.conf` file is for your own additions to the OHS configuration; it will never be overwritten by AutoConfig.

Note that since the rules in `trusted.conf` is basically a blocklist, the slash "/" characters will have to dealt with using regular expressions; i.e. "/" is written as "(/)+". This is to avoid trivial blocklist bypasses, for example if `/OA_HTML/secret2.jsp` is blocked, a URL `/OA_HTML//secret2.jsp`would not match, and thus would not be blocked, but would still call `/OA_HTML/secret2.jsp`.

For more information, refer to My Oracle Support Knowledge Document 387859.1, *Using AutoConfig to Manage System Configurations with Oracle Applications Release 12*.

Network

WLS Network Security

If your network topology and/or load balancer configuration allows direct access to the WebLogic Server (WLS) ports, follow these instructions to reduce the WLS attack surface:

- Only Allow Access to Oracle WebLogic Server Administration Ports from Trusted Hosts, *Oracle E-Business Suite Setup Guide*
- Only Allow Direct Access to Oracle WebLogic Server from Trusted Hosts, *Oracle E-Business Suite Setup Guide*
- Disabling Web Services Atomic Transactions, *Oracle E-Business Suite Setup Guide*

10

Oracle E-Business Suite Security

About Oracle E-Business Suite Security

This section contains security recommendations for configurations within Oracle E-Business Suite.

Hardening

Hardening the Operating Environment

Follow the hardening instructions for Operating Environment Security, page 12-1.

Setting Workflow Notification Mailer SEND_ACCESS_KEY to N

When `SEND_ACCESS_KEY` is set to 'Y', the workflow notification email bypasses the Oracle E-Business Suite sign-on process; email notifications contain an access key. The key allows the user to access the Notification Details web page directly without authenticating. Set `SEND_ACCESS_KEY` to N to prevent inclusion of the key with the Notification Detail link. When set to 'N', an unauthenticated user who clicks on the notification link must sign on before accessing the Notification Details web page.

For more information, refer to the *Oracle Workflow Administrator's Guide*.

Ensuring You Know Who is a Workflow Admin

Verify the setting in WF_RESOURCES to see who workflow considers a workflow administrator:

```
select TEXT from WF_RESOURCES where NAME = 'WF_ADMIN_ROLE' ;
```

Ensure that the value is not set to "*" which means that everybody is a workflow administrator.

Setting Tools Environment Variables

You should prevent forms users from using the enter-query feature on a production system.

In Oracle E-Business Suite Release 12, the Forms parameters are set in the configuration file:

```
/x/inst/apps/VIS12_dbs01/ora/10.1.2/forms/server/default.env
```

Forms Environment Variable	Value
FORMS_RESTRICT_ENTER_QUERY	TRUE

Securing Attachments

Utilize the profile options described in the following sections to secure attachments. In addition to the information below, see My Oracle Support Knowledge Document 1357849.1, *Security Configuration Mechanisms in the Attachments Feature in Oracle E-Business Suite*, for more details.

File Download

Profile option FND: Security File Download Time Limit (FND_GFM_ACCESS_DURATION) specifies the maximum length of time (in minutes) for accessing a Generic File Manager (GFM) file download URL. It was introduced in the July 2019 Oracle E-Business Suite Critical Patch Update (CPU).

The GFM file download URL is most commonly generated when downloading an attachment file or performing an export from an Oracle Form or Oracle Application Framework page. The default value of the profile is five minutes. The five minutes begin when the download URL is initially generated. This download URL cannot be accessed beyond the allotted five minutes. However, once the access is authenticated, the download itself can take as much time as needed.

To set the FND: Security File Download Time Limit profile option, see: "Setting Profile Options" in the *Oracle E-Business Suite Setup Guide*.

Upload File Size Limit

Profile option Upload File Size Limit (UPLOAD_FILE_SIZE_LIMIT) specifies the maximum allowable file size in KB for uploaded attachments for Oracle Application Framework and core attachments. This profile option is set with a default value of 4194304 KB (4GB) at the Site level.

For example, if you set the profile option value to 2000KB (2MB) and try to upload a file that exceeds this value, an error message similar to the following is displayed:

```
    The file you are trying to upload has exceeded the maximum size of
2000 KB. Please upload a file of size less than 2000 KB or contact your
Systems Administrator for assistance.
```

To address this error, set the value of the Upload File Size Limit profile option to a value that matches the size of the file to upload.

Note that for particular iRecruitment responsibilities, this profile option is more restrictive. Other levels may be set so if there are issues uploading a file due to size, the profile should be checked at all levels.

See My Oracle Support Knowledge Document 1357849.1, *Security Configuration Mechanisms in the Attachments Feature in Oracle E-Business Suite*.

To set the Upload File Size Limit profile option, see: "Setting Profile Options" in the *Oracle E-Business Suite Setup Guide*.

File Type Validation

The File Type Validation feature was originally delivered in the Oracle E-Business Suite October 2011 Critical Patch Update (CPU) and updated in subsequent CPUs.

Before this change, users could upload any file type without restrictions. With this enhancement, users will be limited as to what file types of attachments they can upload. File types can be explicitly allowed.

With File Type Validation enabled, users receive an error message when attempting to upload a single file with a restricted file type: "This file type is not allowed. Please choose another file." This feature applies when uploading attachments through the user interface (using the Generic File Manager). Bulk file uploads by administrators will not be restricted.

File types are defined in the fnd_mime_types table. The combination of Media Type (formerly known as MIME type) and file extension uniquely identifies a file type. File types with 'N' for the column ALLOW_FILE_UPLOAD value are explicitly disallowed, as listed in the following table:

Disallowed File Types

Media (MIME) Type	File Extension	ALLOW_FILE_UPLOAD column value
application/jsp	jsp	N
application/octet-stream	wsh	N
application/octet-stream	jse	N
application/octet-stream	class	N

Media (MIME) Type	File Extension	ALLOW_FILE_UPLOAD column value
application/octet-stream	bin	N
application/octet-stream	exe	N
application/octet-stream	com	N
application/octet-stream	bat	N
application/octet-stream	cmd	N
application/octet-stream	wsf	N
application/octet-stream	vbe	N
application/octet-stream	vbs	N
application/x-javascript	js	N
application/x-shockwave-flash	swf	N
application/x-java-archive	jar	N

The restriction on file types is also controlled by the profile option Attachment File Upload Restriction Default (FND_SECURITY_FILETYPE_RESTRICT_DFLT). This profile option determines whether a file type is allowed or not. The values for this profile option are as follows:

- **Yes**: This is the default value on the site level. When the profile option is set to 'Yes', all file types except those with ALLOW='N' can be uploaded. That is, only file types in which the ALLOW flag is not explicitly set to 'N' in fnd_mime_types are allowed to be uploaded, as the fnd_mine_types table acts as a blocklist.

- **No**: When the profile option is set to 'No', only file types with ALLOW='Y' can be uploaded. That is, only file types in which the ALLOW flag are explicitly set to 'Y' in fnd_mime_types are allowed to be uploaded, as the fnd_mime_types table acts as an allowlist.

- **NULL**: If this profile option is NULL for any reason (or does not exist), then the default is to allow uploads (same as the value 'Yes').

Because a file extension can exist in the fnd_mime_types table multiple times (because the combination of mime type and file extension uniquely identifies a file type), the most restrictive value will be used.

For example, say we have the values listed in the following table:

Example Values

MIME Type	File Extension	ALLOW_FILE_UPLOAD column value
application/gzip	gzip	Y
application/x-gzip	gzip	N

In this example, files with the extension "gzip" will be restricted from upload.

How to Modify the List of File Types Allowed/Disallowed

To change what file types are explicitly allowed and disallowed in the fnd_mime_types table, use the APIs as follows.

The package fnd_file_mime_types_pkg is provided to allow the administrators to insert, update, or delete from the fnd_mime_types table. Note that if you are changing a file type from disallowed to allowed, set the Allowed flag to 'Y'.

Here is the syntax of the procedures:

```
PROCEDURE INSERT_ROW (X_ROWID in out nocopy VARCHAR2,
                      X_MIME_TYPE in VARCHAR2,
                      X_CP_FORMAT_CODE in VARCHAR2 DEFAULT NULL,
                      X_CTX_FORMAT_CODE in VARCHAR2 DEFAULT 'IGNORE',
                      X_CREATION_DATE in DATE DEFAULT SYSDATE,
                      X_CREATED_BY in NUMBER DEFAULT NULL,
                      X_LAST_UPDATE_DATE in DATE DEFAULT NULL,
                      X_LAST_UPDATED_BY in NUMBER DEFAULT NULL,
                      X_LAST_UPDATE_LOGIN in NUMBER DEFAULT NULL,
                      X_FILE_EXT in VARCHAR2 DEFAULT NULL,
                      X_ALLOW_FILE_UPLOAD in VARCHAR2 DEFAULT NULL);

PROCEDURE UPDATE_ROW (X_MIME_TYPE_ID in NUMBER,
                      X_MIME_TYPE in VARCHAR2 DEFAULT NULL,
                      X_CP_FORMAT_CODE in VARCHAR2 DEFAULT NULL,
                      X_CTX_FORMAT_CODE in VARCHAR2 DEFAULT NULL,
                      X_LAST_UPDATE_DATE in DATE DEFAULT SYSDATE,
                      X_LAST_UPDATED_BY in NUMBER DEFAULT NULL,
                      X_FILE_EXT in VARCHAR2 DEFAULT NULL,
                      X_ALLOW_FILE_UPLOAD in VARCHAR2 DEFAULT NULL);

PROCEDURE DELETE_ROW (X_MIME_TYPE in VARCHAR2,
                      X_FILE_EXT in VARCHAR2);

PROCEDURE SET_FILE_EXT (X_MIME_TYPE IN VARCHAR2,
                        X_FILE_EXT IN VARCHAR2);
                        X_LAST_UPDATE_DATE in DATE DEFAULT SYSDATE,
                        X_LAST_UPDATED_BY in NUMBER DEFAULT NULL);

PROCEDURE SET_ALLOW_UPLOAD (X_FILE_EXT IN VARCHAR2,
                            X_MIME_TYPE IN VARCHAR2,
                            X_ALLOW_FILE_UPLOAD IN VARCHAR2,
                            X_LAST_UPDATE_DATE in DATE DEFAULT SYSDATE,
                            X_LAST_UPDATED_BY in NUMBER DEFAULT NULL);
```

Examples

To insert a row into the fnd_mime_types table:

```
FND_FILE_MIME_TYPES_PKG.insert_row(x_rowid => xrow,
                                   x_mime_type =>
'application/mime_value',
                                   x_created_by => <userid>,
                                   x_last_updated_by => <userid>,
                                   x_file_ext => 'ext',
                                   X_ALLOW_FILE_UPLOAD => 'N');
```

To allow file upload:

```
FND_FILE_MIME_TYPES_PKG.set_allow_upload(x_file_ext => 'ext',
                                         x_mime_type =>
'application/mime_value',
                                         x_allow_file_upload => 'Y');
```

To use the API fnd_file_mime_types_pkg.update_row first determine the mime_type_id of the record to be updated:

```
execute FND_FILE_MIME_TYPES_PKG.update_row(x_mime_type_id => 82,
X_ALLOW_FILE_UPLOAD => 'Y');
```

> **Note:** If changes do not immediately take effect, a stop and restart of the application tier may be required.

AntiSamy Check

The AntiSamy Check feature was originally delivered in the Oracle E-Business Suite October 2011 Critical Patch Update (CPU) and updated in subsequent CPUs.

This enhancement leverages the AntiSamy libraries to validate HTML files that are uploaded using the Attachment or File Upload features. For more information on the AntiSamy Project, see the Open Web Application Security Project (OWASP) AntiSamy Project page at https://wiki.owasp.org/index.php/Category:OWASP_AntiSamy_Project.

This AntiSamy Check is available for both Oracle Application Framework and Oracle Application Object Library Attachment/File Upload functionality.

The feature is controlled by profile FND: Disable AntiSamy Filter (FND_DISABLE_ANTISAMY_FILTER). When this profile is set to 'No' (the default value), Oracle E-Business Suite will upload a cleaned-up version of a file with the message "The document you uploaded has been modified to remove restricted tags. Please check the document and replace it if necessary." The internal name of this message is FND_CLEAN_DOCUMENT_UPLOAD.

The AntiSamy check uses the policy file named `fnd-antisamy-irec-1_3.xml` under `$JAVA_TOP/policies/antisamy`. See the documentation for AntiSamy if you wish to restrict or relax the HTML tags that are allowed. See My Oracle Support Knowledge Document 122452.1, *Global Customer Services Customization Guidelines*.

HTML Attachment/Uploading with AntiSamy HTML Sanitizing

AntiSamy HTML sanitizing logic parses the uploaded/attached HTML as a string and removes the malicious pieces of code from it. Oracle E-Business Suite assumes the character encoding of the HTML file as follows:

1. Character encoding written in the content-type meta tag in the HTML file.

   The HTML file should have a meta tag to specify the HTML character encoding like the following example:

   ```
   <meta http-equiv="content-type" content="text/html;charset=utf-8" />
   ```

   The character encoding name for this meta tag must be an IANA character encoding name.

2. FND_NATIVE_CLIENT_ENCODING profile option value.

   If Oracle E-Business Suite cannot detect the character encoding from an HTML meta tag, it will get it from the profile option and assume it is equivalent to that of the HTML file.

To avoid the non-ASCII character corruption in HTML by AntiSamy HTML sanitizing, make sure the HTML file being uploaded has a "content-type" meta tag with the right character encoding. If corrupted characters are seen in an uploaded/attached file, check if the HTML is well-formed and has a meta tag for character encoding. The character encoding detection may fail in the following circumstances:

- No character encoding information is specified in a meta tag.
- A meta tag does not exist in `<head>` section.
- `<head>` or `</head>` tag is missing.
- Failure to parse the meta tag because the HTML is malformed. For example, the meta tag does not start with "<" or does not end with ">" or "/>".

When there are multiple "content-type" meta tags in one HTML file, the very first one is used. If it fails to parse the very first one, the character encoding detection logic assumes there is no valid character encoding information in the HTML. The rest of the "content-type" meta tags will not be parsed.

If the character encoding cannot be described in an HTML "content-type" meta tag for some reason, use the FND_NATIVE_CLIENT_ENCODING profile option value to specify the HTML character encoding. Note that the value of FND_NATIVE_CLIENT_ENCODING is generally referred in text file uploading, downloading, and data exporting; and not for HTML file uploading/attachment only. Thus, the FND_NATIVE_CLIENT_ENCODING value must be set carefully.

Allowed Attachment Protocols

Profile option FND: Attachment URL Allowed Protocols (FND_ATTACHMENT_ALLOWED_PROTOCOLS) contains a comma-separated list of protocols that are allowed for Attachment URLs.

The default value is `https,http`.

Use this profile to specify which protocols are allowed for Attachment Web documents. If a user attempts to open an Attachment Web page with a protocol that is not in the list, an error message is displayed.

For more information on the FND: Attachment URL Allowed Protocols profile option, see "Setting Profile Options" in the *Oracle E-Business Suite Setup Guide*.

Internet Content Adaptation Protocol (ICAP) Antivirus Software Configuration

You can choose which antivirus software to use to scan attachments files and file uploads in Oracle Application Framework and Oracle Forms applications. For more information, see: Internet Content Adaptation Protocol (ICAP) Antivirus Software Configuration, *Oracle E-Business Suite Setup Guide*.

Optional Secure Configurations

Security policy must balance risk of attack, cost of defense and value of data protected. This section contains recommendations that improve security, but may not be appropriate for every deployment.

Encrypting Credit Cards

The technical reference paper in My Oracle Support Knowledge Document 1573912.1, *All About Oracle Payments Release 12 Wallets And Payments Data Encryption*, describes the credit card encryption features available in Oracle E-Business Suite. The feature is part of Release 12, but needs to be explicitly turned on.

Encryption of credit card numbers is one of many requirements for PCI PA-DSS compliance.

Practicing Safe Cloning

In many production environments, it is part of normal operational procedure to periodically create clones (copies) of production databases for various purposes. These copies are typically used for performance test by DBAs or developers or to test upgrade/patching of the production database.

When these cloned copies of production databases are to be used outside the group of trusted production administrators, there will be concerns about the confidentiality of the data contained in the database as data scrambling routines are typically run on the cloned copy before it is handed over to development. The data scrambling protects the confidentiality of production data such as employee data (Name, Address, Social Security Number, Compensation details) customer data (Name, Address, Credit Card info) and other data considered confidential.

To ensure the integrity of the production database you must also change all the passwords in the clone to ensure that it will not be possible to retrieve passwords from the cloned instance that could be used to compromise the production database either by gaining administrative access or by allowing someone to impersonate another user.

See My Oracle Support Knowledge Document 419475.1, *Removing Credentials from a Cloned EBS Production Database*, for an example of how to remove production credentials and bootstrap new credentials in a cloned copy of your production database. The steps in Document 419475.1 should be incorporated in your local cloning procedures.

Network

Using Certified HTTP Security Headers

A server can pass additional information with a response using HTTP headers. HTTP security headers can provide additional protection against attacks and security vulnerabilities.

The following table lists HTTP security response headers that are certified for use with Oracle E-Business Suite.

Certified HTTP Security Headers for Oracle E-Business Suite

HTTP Header	Description	Oracle E-Business Suite Configuration and Reference
X-Frame-Options: `SAMEORIGIN`	Response header to avoid clickjacking attacks by preventing other sites from embedding (framing) your content.	In Oracle E-Business Suite Release 12.2, we introduced protections against clickjacking by setting the X-Frame-Options HTTP header for all pages. This is enabled by default with the following configuration line in the Oracle HTTP Server (OHS) `oracle_apache.conf` file: `Header set X-Frame-Options SAMEORIGIN` **Note:** If you require the ability to frame Oracle E-Business Suite pages from a site other than the Oracle E-Business Suite site, you may have to temporarily disable this header while working on a permanent solution (such as by rehosting or proxying). To temporarily disable the header, comment out the entry in the `httpd.conf` file and restart OHS.
X-Content-Type-Options: `nosniff`	Response header that prevents browsers from attempting to guess the MIME type of a file by looking at its content.	As of the October 2018 Critical Patch Update (CPU), this configuration is enabled by default. See My Oracle Support Knowledge Document 2445688.1, *Oracle E-Business Suite Release 12 Critical Patch Update Knowledge Document (October 2018)*, for more information on the October 2018 CPU.

HTTP Header	Description	Oracle E-Business Suite Configuration and Reference
Strict-Transport-Security (HTTP Strict Transport Security)	Response header that specifies that the site should only be contacted using HTTPS.	In Oracle E-Business Suite Release 12.2, we introduced manual configuration to enable HSTS. For additional information regarding HSTS, refer to My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*. **Caution:** We recommend that you implement the HSTS only after testing that it does not break any customized code or third-party integrations.
Cookie Domain Scoping	Code that specifies the scope of where the browser will send the cookie.	In Oracle E-Business Suite Release 12.2, we introduced a configuration option for the domain attribute for the Oracle E-Business Suite ICX session cookie. Manual configuration is required to use this feature. See the Cookie Domain Scoping, page 4-79 section for additional information.

HTTP Header	Description	Oracle E-Business Suite Configuration and Reference
`secure` Cookie Attribute	A Set-Cookie response header attribute that prevents cookies from being sent with non-HTTPS requests.	**ICX Session Cookie** If you have enabled TLS for Oracle E-Business Suite, the secure cookie attribute is automatically added to the ICX session cookie (also known as the Oracle E-Business Suite session cookie) by default. TLS enablement for Oracle E-Business Suite is required for this configuration. For more information, see My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*. **JSESSIONID Cookie** The JSESSIONID cookie is a generic Java session cookie set by the Oracle Applications Server. If your Oracle E-Business Suite web entry point is using HTTPS, follow the instructions in Configure the JSESSIONID Cookie, page 10-15.

HTTP Header	Description	Oracle E-Business Suite Configuration and Reference
`httpOnly` Cookie Attribute	A Set-Cookie response header attribute that prevents client side script from accessing the cookie.	**ICX Session Cookie** The HTTPOnly cookie attribute is set automatically for the ICX session cookie (also known as the Oracle E-Business Suite session cookie) when the following minimum requirements are met: • The application of R12. ATG_PF.C.Delta.7. • The enablement of the Java Web Start option for running Forms for Oracle E-Business Suite. Refer to the following for additional information: • Readme for R12.ATG_PF. C.Delta.7. • My Oracle Support Knowledge Document 2188898.1, *Using Java Web Start with Oracle E-Business Suite*, for how to implement Java Web Start with Oracle E-Business Suite. **JSESSIONID Cookie** The JSESSIONID is a generic Java session cookie set by the Oracle Applications Server. If you have enabled the Java Web Start option for running Forms for Oracle E-Business Suite, follow the instructions in Configure the JSESSIONID Cookie, page 10-15.

HTTP Header	Description	Oracle E-Business Suite Configuration and Reference
`samesite` Cookie Attribute	A Set-Cookie response header attribute that mitigates the risk of cross-site request forgery (CSRF) and information leakage attacks by asserting that the cookie should only be sent with requests initiated from the same registrable domain.	Patch 29672027:R12.TXK.C delivers context file parameters to enable and configure the SameSite cookie attribute. The parameters control the SameSite attributes for all cookies set from the HTTP entry point. After applying Patch 29672027, the default value of the SameSite cookie attribute (s_samesite_cookie_enabled) is set to # which disables the attribute. To enable the SameSite cookie attribute, you must set the value to "blank" as follows: `s_samesite_cookie_enable=""` You can also set the context variable s_samesite_cookie_attribute to 'strict' or 'lax'. By default, s_samesite_cookie_attribute is set to strict. For additional information, refer to: https://tools.ietf.org/html/draft-west-first-party-cookies-07. If Oracle Access Manager and your Oracle E-Business Suite system do not reside on the same domain, you will need to set the context variable s_samesite_cookie_attribute to 'lax'. If you are using iProcurement and plan to enable the SameSite cookie attribute, you must also apply Patch 31259179:R12.ICX.D and Patch 31840095:R12.FND.C. Based on the ATG level you

HTTP Header	Description	Oracle E-Business Suite Configuration and Reference
		are on, you may need to apply an FND one-off patch along with the iProcurement patch. • If you are on R12.ATG_PF.C.Delta.7 or later, apply Patch 29705896:R12.FND.C. • If you are on R12.ATG_PF.C.Delta.6, manually add `/OA_HTML/jsp/icx/punchout/PunchoutCallBack.jsp` to `allowed_jsps_Procurement.conf`. • If your R12.ATG Release Update Pack level is older than R12.ATG_PF.C.Delta.6, no additional FND patch is required. When enabling the SameSite cookie attribute, make sure to test integrations that are deployed in domains that differ from the Oracle E-Business Suite domain. A few examples of integrations that may have a different domain include iProcurement punchout or single sign-on integration with Oracle Access Manager or Identity Cloud Service.

Configure the JSESSIONID Cookie

You should configure the JSESSIONID cookie if both of the following conditions are true:

- The Oracle E-Business Suite web entry point is using HTTPS.

- Java Web Start is enabled for running Forms on Oracle E-Business Suite.

Use the following sections to configure the JSESSIONID cookie on the OACORE managed server and Forms and the OAFM managed server.

For the OACORE Managed Server

1. Make a backup copy of the configuration in `<EBS_ORACLE_HOME>/deployment_plans/oacore/plan.xml`. You will be making modifications to this file.

2. Find the following entry in the `plan.xml` file:

```
<variable>

<name>WeblogicApplication_SessionDescriptor_CookieHttpOnly</name>
    <value>false</value>
</variable>
```

   And replace it with the following:

```
<variable>

<name>WeblogicApplication_SessionDescriptor_CookieHttpOnly</name>
    <value>true</value>
</variable>
<variable>
    <name>WeblogicApplication_SessionDescriptor_CookieSecure</name>
    <value>true</value>
</variable>
<variable>

<name>WeblogicApplication_SessionDescriptor_UrlRewritingEnabled</nam
e>
    <value>false</value>
</variable>
```

3. Then, find the following entry in the `plan.xml` file:

```
<variable-assignment>

<name>WeblogicApplication_SessionDescriptor_CookieHttpOnly</name>
    <xpath>/weblogic-application/session-descriptor/cookie-http-
only</xpath>
</variable-assignment>
```

   And replace it with the following:

```
<variable-assignment>

<name>WeblogicApplication_SessionDescriptor_CookieHttpOnly</name>
    <xpath>/weblogic-application/session-descriptor/cookie-http-
only</xpath>
</variable-assignment>
<variable-assignment>
    <name>WeblogicApplication_SessionDescriptor_CookieSecure</name>
    <xpath>/weblogic-application/session-descriptor/cookie-
secure</xpath>
</variable-assignment>
<variable-assignment>

<name>WeblogicApplication_SessionDescriptor_UrlRewritingEnabled</nam
e>
    <xpath>/weblogic-application/session-descriptor/url-rewriting-
enabled</xpath>
</variable-assignment>
```

4. Start your application.

5. Retest the configuration.

For Forms and the OAFM Managed Server

1. Make a backup copy of the configuration in `<EBS_ORACLE_HOME>/deployment_plans/forms/plan.xml` and `<EBS_ORACLE_HOME>/deployment_plans/oafm/plan.xml`. You will be making modifications to these files.

2. In each `plan.xml` file, find the following entries:

```
<variable>
    <name>WeblogicApplication_SessionDescriptor_CookieName</name>
    <value>JsessionIDOAFM</value>
</variable>
```

Or

```
<variable>
    <name>WeblogicApplication_SessionDescriptor_CookieName</name>
    <value>JsessionIDForms</value>
</variable>
```

And insert the following content after the entry:

```
<variable>

<name>WeblogicApplication_SessionDescriptor_CookieHttpOnly</name>
    <value>true</value>
</variable>
<variable>
    <name>WeblogicApplication_SessionDescriptor_CookieSecure</name>
    <value>true</value>
</variable>
<variable>

<name>WeblogicApplication_SessionDescriptor_UrlRewritingEnabled</nam
e>
    <value>false</value>
</variable>
```

3. Then, find the following entry in the `plan.xml` file:

```
<variable-assignment>
    <name>WeblogicApplication_SessionDescriptor_CookieName</name>
    <xpath>/weblogic-application/session-descriptor/cookie-
name</xpath>
</variable-assignment>
```

And insert the following content after the entry:

```
<variable-assignment>

<name>WeblogicApplication_SessionDescriptor_CookieHttpOnly</name>
    <xpath>/weblogic-application/session-descriptor/cookie-http-
only</xpath>
</variable-assignment>
<variable-assignment>
    <name>WeblogicApplication_SessionDescriptor_CookieSecure</name>
    <xpath>/weblogic-application/session-descriptor/cookie-
secure</xpath>
</variable-assignment>
<variable-assignment>

<name>WeblogicApplication_SessionDescriptor_UrlRewritingEnabled</nam
e>
    <xpath>/weblogic-application/session-descriptor/url-rewriting-
enabled</xpath>
</variable-assignment>
```

Using TLS to Encrypt Oracle E-Business Suite Connections

Information sent over the network and across the internet in clear text may be intercepted. Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) are features that provide encryption of network traffic between the user's browser and the Oracle E-Business Suite web server. You should configure your Oracle E-Business Suite environment to use TLS for all inbound (HTTP), outbound, and loopback connections.

If you are enabling encryption for Oracle E-Business 12.2 for the first time, follow the instructions in My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*.

As of October 2014, all versions of SSL are insecure and should not be used. Oracle highly recommends that Oracle E-Business Suite customers migrate from SSL to TLS 1.2. Migrating to TLS 1.2 will address recent security vulnerabilities (such as POODLE, FREAK, Logjam, and RC4 NOMORE). If you are migrating from SSL to TLS, follow the instructions in My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*.

Avoiding Weak Ciphers and Protocols for SSL (HTTPS)

You should avoid all cipher suites with a key size less than 128-bit and any RC4-based cipher suite to avoid security vulnerabilities.

For more information, see My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2*.

Using External Web Tier if Exposing Any Part of Oracle E-Business Suite to the Internet

If you expose any part of your Oracle E-Business Suite production system to the internet, you should consult My Oracle Support Knowledge Document 1375670.1, *Oracle E-Business Suite Release 12.2 Configuration in a DMZ*, for our advice for deploying external Oracle E-Business Suite products to the internet. This document describes the role of DMZs, external web tiers, external responsibilities, URL firewall, and reverse proxies in a secure external Oracle E-Business Suite deployment.

Using Terminal Services for Client-Server Programs

Deploy client/server components requiring direct connection to the Oracle E-Business Suite production database on secured, trusted servers rather than on end user desktop machines.

The majority of the Oracle E-Business Suite functionality available to end users does not require direct database access but is web-based. Web browser sessions connect to application tier servers running Oracle Fusion Middleware. The application tier servers then make the database connections.

If you have a well considered need to connect to the production database directly from a desktop, deploy a remote server environment based on Windows Server Terminal Services, Citrix, or Tarantella (now Oracle Secure Global Desktop).

The challenge is to make the server running the client/server program a trusted server. If the end user is running with administrator or power-user privileges, or has physical access to the host, it does not qualify as "trusted."

If the client/server tool uses DBC files these DBC files must be protected from the user while ensuring that the program run by the user has read access to the DBC file.

Further details are provided in the following sections: Add IP Restrictions / Enable Valid Node Checking, page 7-5, Activate Server Security, page 10-27, and Create DBC Files Securely, page 10-28.

Authentication

Changing Passwords for Seeded Application User Accounts

Oracle ships seeded user accounts with default passwords. Change the default passwords immediately. Depending on product usage, some seeded accounts can or can not be disabled. Disable an application user account by setting the END_DATE for the account.

- Do not disable the `GUEST` user account.
- Do not disable the `SYSADMIN` user account until you have created other accounts

with similar privilege.

Note that we ship a script named `fnddefpw.sql`. If you run this script as APPS, it will list the seeded accounts that still have the default password.

The following table lists the application users shipped with Oracle E-Business Suite Release 12 and indicates:

- If it has a default password, you should **Change**
- If you can safely **Disable** the account (if not used by your product mix)
- If the account ships an impossible password (**NoPwd**)
- If the account ships disabled (**EndDT**)

See description of the columns after the table and notice the footnotes following the table.

Application Users Shipped with Oracle E-Business Suite Release 12

Account	Product/Purpose	Change	Disable	NoPwd	EndDT
AME_INVALID_APPROVER	AME WF migration 11.5.9 to 11.5.10	Y	Y		
ANONYMOUS	FND/AOL - Anonymous for non-logged users	Y	Y		x
APPSMGR	Routine maintenance via concurrent requests	N	Y	x	x
ASADMIN	Application Server Administrator	N	Y	x	x

Account	Product/Purpose	Change	Disable	NoPwd	EndDT
ASGADM	Mobile gateway related products	Y	Y(a)		
ASGUEST	Sales Application guest user	Y	Y(b)		
AUTOINSTALL	AD	Y	Y		
CONCURRENT MANAGER	FND/AOL: Concurrent Manager	Y	Y		x
FEEDER SYSTEM	AD - Supports data from feeder system	Y	Y		x
GUEST	Guest application user	Y(c)	N		
IBE_ADMIN	iStore Admin user	Y	Y(d)		
IBE_GUEST	iStore Guest user	Y	Y(d)		
IBEGUEST	iStore Guest user	Y	Y(d)		
IEXADMIN	Internet Expenses Admin	Y	Y		
INDUSTRY DATA		N	Y	x	

Account	Product/Purpose	Change	Disable	NoPwd	EndDT
INITIAL SETUP	AD	Y	Y		x
IRC_EMP_GUEST	iRecruitment Employee Guest Login	Y	Y		
IRC_EXT_GUEST	iRecruitment External Guest Login	Y	Y		
MOBILEADM	Mobile Applications Admin	Y	Y		
MOBILEDEV	Mobile Applications Development	Y	Y		
OP_CUST_CARE_ADMIN	Customer Care Admin for Oracle Provisioning	Y	Y		
OP_SYSADMIN	OP (Process Manufacturing) Admin User	Y	Y		
ORACLE12.[0-9].0	Owner for release specific seed data	N	N	x	
PORTAL30	Desupported Portal 3.0.x Account	Y	Y		
PORTAL30_SSO	Desupported Portal 3.0.x Account	Y	Y		

Account	Product/Purpose	Change	Disable	NoPwd	EndDT
STANDALONE BATCH PROCESS	FND/AOL	Y	Y		
SYSADMIN	Application Systems Admin	Y	N		
WIZARD	AD - Application Implementation Wizard	Y	Y		
XML_USER	Gateway	Y	Y		

(a) Required for Mobile Sales, Service, and Mobile Core Gateway components.

(b) Required for Sales Application.

(c) If the GUEST password is changed, set the AutoConfig variable s_guest_pass to the new value in the context file before running AutoConfig. AutoConfig must be run to propagate the new password to config files.

> **Note:** The GUEST password must always be in UPPERCASE.

(d) Required for iStore.

In the table, an 'x' in the EndDT column means the account ships end-dated.

In the table, an 'x' in the NoPwd column indicates that the account ships with an "impossible password," this means that the password column in FND_USER contains a clear text string that is never a valid encrypted or hashed password. Thus it is not possible to login as this user, unless you change the password.

The "impossible" value can be "DUMMY," "INVALID," or "INTERNAL USER-NOLOGIN."

> **Note:** If the "impossible" value is not "INVALID", FNDCPASS will log a "cannot decrypt" error which can be ignored. More recent R12 versions consistently use "INVALID."

You can easily identify the users with an impossible password as the length of the impossible password is shorter than the encrypted or hashed password. For example, this SQL statement will list users with an impossible password:

```
select USER_NAME,END_DATE,ENCRYPTED_USER_PASSWORD from FND_USER
   where length(ENCRYPTED_USER_PASSWORD)<30 order by 1;
```

In the table, a 'Y' in the Change column indicates that you should change the password for the account as it ships with a default password. A value of 'N' means that you do not have to change anything to get rid of a default password. If the account is used by your Oracle E-Business Suite product mix, you should change the default password to a password of your choosing, and according to the implementation guide for the product that requires it.

Switching to Hashed Passwords

Traditionally, Oracle E-Business Suite has stored the password of the application users (FND_USERs) in encrypted form. Starting with release 12.0.4, it is possible to switch the Oracle E-Business Suite system to store hashed versions of the passwords instead.

To switch Oracle E-Business Suite to use hashed passwords, you must use the AFPASSWD command-line utility in MIGRATE mode. See the *Oracle E-Business Suite Maintenance Guide* for more details.

> **Note:** This process is irreversible.

Tightening Logon and Session Profile Options

For local application users, the profile option settings below support strong passwords, account lockout after too many failed logons, and session inactivity timeout.

Recommended Values for Tightening Logon and Session Profile Options

Profile Option Internal Name	Recommended Value
SIGNON_PASSWORD_LENGTH	8
SIGNON_PASSWORD_HARD_TO_GUESS	YES
SIGNON_PASSWORD_NO_REUSE	180
SIGNON_PASSWORD_CASE	Sensitive
SIGNON_PASSWORD_FAILURE_LIMIT	5(a)
ICX_SESSION_TIMEOUT	30
SIGNON_PASSWORD_CUSTOM	implement(b)

(a) Setting automatic account locking after N failed attempts make for a simple denial of service attack. If you set this profile option monitor the FND_UNSUCCESSFUL_LOGINS table.

(b) If your corporate password policy cannot be expressed using the above parameters, you may implement a custom password validation function and register it with Oracle E-Business Suite. See Customizing Password Validation, page 10-25.

Optional Secure Configurations

Security policy must balance risk of attack, cost of defense and value of data protected. This section contains recommendations that improve security, but may not be appropriate for every deployment.

Customizing Password Validation

If your corporate password policy cannot be expressed using the "Sign-On" parameters as found in Tighten Logon and Session Profile Options, page 10-24, you can implement a custom function for validating new passwords.

To customize password validation create a Java class that implements the `oracle.apps.fnd.security.PasswordValidation` Java interface. The interface requires three methods:

1. `public boolean validate(String user, String password`

   This method takes a user name and password, and returns True or False, indicating whether the user's password is valid or invalid, respectively.

2. `public String getErrorStackMessageName()`

   This method returns the name of the message to display when the user's password is deemed invalid (for example, the validate() method returns False).

3. `public String getErrorStackApplicationName()`

   This method returns the application short name for the aforementioned error message.

After writing the customized password validator, set profile option `SIGNON_PASSWORD_CUSTOM` to the full name of the class. If the name of the Java class is `yourco.security.AppsPasswordValidation`, then the value of `SIGNON_PASSWORD_CUSTOM` must be "`yourco.security.AppsPasswordValidation`". Note, this class must be loaded into the Application database using the `loadjava` command.

Creating New User Accounts Safely

Oracle User Management (UMX) provides a common user registration flow in which a user can enter a new password or select to have one generated randomly. UMX uses workflow to drive the registration process once a request has been submitted. See UMX

documentation for more details.

Creating Shared Responsibilities Instead of Shared Accounts

When users share one account, the system cannot identify which user performs a function, preventing accountability. Users share the same functions or permission sets, while the system tracks individual user actions.

Configuring Concurrent Manager for Safe Authentication

Concurrent manager passes the APPS schema password to concurrent programs on the command line. Because some operating systems allow all machine users to read a program's command line arguments, the password may be intercepted. To prevent this, define the concurrent program executable as a HOST program in the concurrent program executable form. Enter `ENCRYPT` in the Execution Options field of the concurrent programs window when defining a concurrent program using this executable. ENCRYPT signals the concurrent manager to pass the user name/password in the environment variable FCP_LOGIN. Concurrent manager leaves argument $1 blank.

To prevent the user name/password from being passed, enter `SECURE` in the Execution Options field. With this change, concurrent manager does not pass the user name/password to the program. This means that the program will have to get the database credentials some other way if it needs to connect to the database.

Configuring Concurrent Manager for Start and Stop Without the APPS Password

Traditionally, the operator starting and stopping the application services needed to know the APPS user name and password in order to start the application services on an application tier that was running the concurrent manager.

Starting with Oracle E-Business Suite Release 12.1.3, it is possible to create an applications user (FND User) with the responsibility Concurrent Manager Operator and use this user's user name and password start and stop the application services.

This is implemented by:

- Creating a new user (for example, CONCOPER) and assigning the "Concurrent Manager Operator" responsibility to this user
- On the application tier, update the following 4 variables in the AutoConfig context file:

AutoConfig Variables to Update

AutoConfig Variable	New Value
s_cp_user	CONCOPER (or the one you created)
s_cp_password_type	AppsUser
s_cp_resp_shortname	FND
s_cp_resp_name	Concurrent Manager Operator

- Run AutoConfig on the application tier(s)

Following this change, the application tier services can be started and stopped by calling `adstrtal.sh` and `adstpall.sh` with the `-secureapps` option and the script will prompt for the Application user's user name and password rather than the APPS user name and password.

For example:

```
[applmgr@app01]$ adstrtal.sh -secureapps

Enter the Applications username: CONCOPER
Enter the Applications password:
```

Activating Server Security

Oracle E-Business Suite Release 12 is deployed in a multi-tier configuration with one database server and an application tier with many possible application servers. The application servers include Apache JSP/Servlet, Forms, Discoverer. Any program which makes a SQLNet connection to the Oracle Applications database needs to be trusted at some level. The Server Security feature ensures that FNDLogin connections originate from trusted machines.

> **Additional Information:** Concerning Oracle Discoverer, see also My Oracle Support Knowledge Document 2277369.1, *Oracle E-Business Suite Support Implications for Discoverer 11gR1*.

Setting Up Server Security

The Application Server Security feature is activated by default, all you should do is verify that the setting is set to SECURE.

This setting is controlled by the AutoConfig variable `s_appserverid_authentication`.

Application Server Security has three states:

- **OFF** - Inactivates Server Security. Server and code IDs are not checked. Appropriate for machines completely under an administrator's control. OK for development systems without production data.
- **ON** - Equivalent to OFF from a security perspective. Not recommended for production systems.
- **SECURE** - Recommended; only registered application servers and trusted code modules may connect.

Checking Server Security Status

Check the Server Security status using the `STATUS` command in the AdminAppServer utility before activating server security to ensure that all desired application servers have been registered. For details, see: Administering Server Security, *Oracle E-Business Suite Setup Guide*, *Oracle E-Business Suite Setup Guide*.

Another way to verify that server security is set to secure is to run the following SQL query while connected as APPS:

```
SQL> select NODE_NAME,SERVER_ID,SERVER_ADDRESS from FND_NODES
     where SERVER_ADDRESS = '*' ;

NODE_NAME      SERVER_ID     SERVER_ADDRESS
-------------- ------------- ---------------
AUTHENTICATION SECURE        *
```

Creating DBC Files Securely

Previous versions of documentation documented how to create DBC files for the Oracle E-Business Suite application tiers using the AdminAppServer utility. Oracle E-Business Suite Release 12 already does this automatically through AutoConfig, so you should never have to do this manually.

However when creating DBC files for use by desktop installations or for other, non-Oracle E-Business Suite application tiers that must connect to the Oracle E-Business Suite database, you must use the AdminDesktop utility to create the DBC file.

Examples of such external hosts are a webservice host or a BPEL service host.

Creating DBC files for these external, non-Oracle E-Business Suite tiers involves:

- Running AdminDesktop on the Oracle E-Business Suite tiers to create the DBC file
- Copying the DBC file to the external tier
- Configuring the external tier to use the DBC file as a data source

Use of `AdminDesktop` - and documentation of any patches needed - can be found in My Oracle Support Knowledge Document 974949.1, *Oracle E-Business Suite Software*

Development Kit for Java.

When creating DBC files make sure to make them IP address specific and that the file permissions are set to 600 (-rw-------).

Consider Using Single Sign-On

Oracle E-Business Suite Release 12 support integration with a Single Sign-On (SSO). For more information on Single Sign-On deployments, refer to My Oracle Support Knowledge Document 376811.1, *Integrating Oracle E-Business Suite Release 12 with Oracle Internet Directory and Oracle Single Sign-On*.

Change Password for WebLogic Server Admin User

Follow the instructions in Changing the Oracle WebLogic Server Administration User Password, *Oracle E-Business Suite Setup Guide* to change the default password for the Oracle WebLogic administration user. The default password should be changed immediately.

Authorization

Reviewing and Limiting Responsibilities and Permissions

Some forms and pages in Oracle E-Business Suite allow a user to modify the functionality of the applications by specifying values such as SQL statements, SQL fragments such as WHERE clauses, HTML strings, and operating system commands or environment variables. These screens may constitute a security risk if used in an unauthorized fashion. Most of these screens are accessible only from system administration menus and responsibilities, where availability should be limited to a very few trusted users. You should eliminate or minimize access to these screens in a production system and know exactly which users have access to these screens.

There are several types of these sensitive pages in Oracle E-Business Suite, and they are controlled by different mechanisms. They can be grouped them into the following categories:

- Oracle Forms Controlled by Function Security
- HTML Pages Controlled by Function Security
- Functionality Controlled by Profile Options
- Pages Controlled by JTF Permissions and Roles

My Oracle Support Knowledge Document 1334930.1, *Sensitive Objects and Administrative Pages in Oracle E-Business Suite*, lists these forms, pages, profile options and includes a description of how to determine who has access by interactively using UMX User

Management or by running SQL scripts.

Setting Other Security-Related Profile Options

Set the recommended values for the security-related profile options as listed in the following table. It is recommended that these settings are applied at site level. In general, the values for the following security-related profile options should not be set to any non-recommended value at any other level than site.

Recommended Security-Related Profile Option Values

Profile Option Name	Code (Internal Name)	Recommended Value	Comments and References
FND: Diagnostics	FND_DIAGNOSTICS	No	The recommended value ensures there are no verbose error messages. The recommended value prevents information leakage and ensures that details of unexpected error messages are not sent to the user. Generally, users should not have this profile option enabled. If required, FND: Diagnostics should only be set at the user level to provide diagnostics to Support.
Utilities:Diagnostics	DIAGNOSTICS	No	See "Utilities: Diagnostics" in the *Oracle E-Business Suite Setup Guide*. If required, this should only be set at the user level. Generally, users should not have this profile enabled.

Profile Option Name	Code (Internal Name)	Recommended Value	Comments and References
Personalize Self-Service Defn	FND_CUSTOM_OA_DEFINITION	No	Only set at user level for users that require this functionality. Generally, users should not have this profile enabled.
Attachment File Upload Restriction Default	FND_SECURITY_FILETYPE_RESTRICT_DFLT	No	The recommended value allows for only file types with ALLOW='Y' to be uploaded. That is, only file types in which the ALLOW flag are explicitly set to 'Y' in fnd_mime_types are allowed for upload. See File Type Validation, page 10-3.
FND: Disable AntiSamy Filter	FND_DISABLE_ANTISAMY_FILTER	No	The recommended value enables AntiSamy checks. See AntiSamy Check, page 10-7.

Profile Option Name	Code (Internal Name)	Recommended Value	Comments and References
Restrict Text Input	FND_RESTRICT_INPUT	Yes	The recommended value enables additional validation of parameters. This profile option provides a defense in depth filter against XSS (Cross Site Scripting) and other HTML injection attacks. When enabled, it invokes an HTML tag filter on input fields and parameters. Test any input fields or parameters in which you expect to be passing HTML or HTML fragments.
BNE Allow No Security Rule	BNE_ALLOW_NO_SECURITY_RULE	No	The recommended value prevents access to global integrators (integrators without a security rule).

Profile Option Name	Code (Internal Name)	Recommended Value	Comments and References
Export Secure Output Format	FND_EXPORT_FORMAT	Space Escape	This profile allows you to define the escape character for exported data to prevent a CSV injection which would allow a lead character to run a macro and corrupt data downloaded to Excel. The recommended value "Space Escape" is the default value. This can be changed to any other value except "Do Not Escape".

Profile Option Name	Code (Internal Name)	Recommended Value	Comments and References
FND: Authn Service Token Scope	FND_AUTHN_SRVC_TOKEN_SCOPE	Header Only	The recommended value for the profile will set the ICX cookie only in the response header of the mLogin REST service and will not return the cookie details in the response payload. If you have custom code that calls the mLogin REST service and the cookie details are required in the response payload, then you must temporarily change the profile value to "Header and Body" to avoid failures when running the custom code. The value "Header and Body" will set the ICX cookie in the header and returns the cookie name and value in the payload. For security and privacy purposes, we recommend that you modify your custom code to retrieve the cookie details from the response header as soon as possible. After your custom code has been updated to meet recommended security standards, you should change

Profile Option Name	Code (Internal Name)	Recommended Value	Comments and References
			the FND: Authn Service Token Scope (FND_AUTHN_SRVC_TOKEN_SCOPE) profile to "Header Only" at the site level.

The Critical Security Profile Values security guideline in the Secure Configuration Console checks these profile options to ensure recommended settings are applied. See Checked Security Guidelines, page 13-3 for more information on this and other security guidelines checked by the Secure Configuration Console.

Restricting Responsibilities by Web Server Trust Level

When web servers have been assigned a server trust level, the system may restrict access to a responsibility based upon that trust level. Three trust levels are supported:

1. Administrative
2. Normal
3. External

Typically, *administrative* web servers are used exclusively by system administrators, are considered secure and have full application access with few limitations. *Normal* web servers are those used by employees within a company's intranet and requiring non-administrative responsibilities. Lastly, customers or employees outside of a company's firewall connect to *external* servers. These have access to a small set of responsibilities.

Setting the Server Trust Level for a Server

To assign a trust level to a web server, the administrator sets the NODE_TRUST_LEVEL profile option. This option, a server-based profile option, can be set to either 1, 2 or 3. The number 1 means administrative, 2 means normal, and 3 means external. To avoid having to set the NODE_TRUST_LEVEL for every single web server, administrators may wish to set the NODE_TRUST_LEVEL profile to some default level of trust at the site level. If no value is set for NODE_TRUST_LEVEL, the web server is assumed to have a trust level of 1 (administrative).

Restricting Access to a Responsibility

When a user logs on to Oracle Applications using a web server, the system determines which responsibilities are valid for that user, and of those responsibilities, which can be

accessed from that particular web server. The system returns only responsibilities appropriate for the web server Trust Level.

To restrict access to a responsibility, set the Application Server Trust Level profile option value for that responsibility to be the number 1, 2 or 3. This indicates that only web servers with the same or greater ordinal trust level may access that responsibility.

For example, a responsibility with an Application Server Trust Level set to 1 (administrative) would only be available if the web server has its Application Server Trust Level set to 1 (administrative), as well. A responsibility with Application Server Trust Level set to 2 (normal) would only be available if the web server has its Server Trust Level set to either 1 (administrative) or 2 (normal).

Profile Option - Application Server Trust Level

Responsibilities or applications with the specified level of trust can only be accessed by an application server with at least the same level of trust. Users can see this profile option, but they cannot update it. The system administrator access is described in the following table:

System Administrator Access Levels

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	No	No

References

For more information on how to enable and use the above security features, refer to Part I of the *Oracle E-Business Suite Security Guide*.

11

Desktop Security

About Desktop Security

This section contains security recommendations for the desktop used to run web browsers that connect Oracle E-Business Suite.

Hardening

Configuring the Browser

See My Oracle Support Knowledge Document 389422.1, *Recommended Browsers for Oracle E-Business Suite Release 12*, for information about securing the desktop.

Updating the Browser

- Update browser when new versions are released; they often include security bug fixes.
- Check browser for built-in safety features.

Updating Java

- Upgrade to Java 8.
- Apply the latest JRE updates.

Turning Off Autocomplete

For kiosk machines, change the browser's autocomplete settings. Although convenient for frequently accessed pages, for privacy and security reasons this feature should be

disabled.

Also consider disabling the "remember password" function, or use a primary password for the saved password store.

Setting Policy for Unattended PC Sessions

People may attempt to access an unattended workstation while another user is still logged into the system. The users should never leave their workstation unattended while logged into the system because it makes the system accessible to others who may walk up to the computer. Organizations should set a corporate policy for handling unattended PC sessions. Users are recommended to use the password-locked screen savers feature on all PCs.

Setting the FileStreaming Security Policy of the No-Store Directive

Use the following profile option to set the FileStreaming security policy for the no-store directive:

Profile Option Name	Code (Internal Name)	Recommended Value
FND: Security FileStreaming No-Store	FND_SEC_FILESTREAM_NO STORE	SECURE

The FND: Security FileStreaming No-Store profile option values are as follows:

- **SECURE** - This value enables Secure mode, where the no-store directive is used to prevent caching for all content. This is the default and recommended profile option value.
- **CHROMIUM_PDF_WA** - This value allows for the caching of PDF content on Chromium-based browsers. Set the profile option to CHROMIUM_PDF_WA when users expect the ability to save PDF content directly from the in-browser PDF viewer.
- **INSECURE** - This value enables Insecure mode and allows the caching of all content.

12

Operating Environment Security

Overview of Operating Environment Security

The environment in which Oracle E-Business Suite runs contributes to or detracts from overall system security. This section contains security recommendations for tightening Oracle file system security along with more general advice for overall system hardening.

Hardening

Cleaning up File Ownership and Access

1. The directory `$ORACLE_HOME/bin` contains Oracle executables. Check that the operating system owner of these executables matches the operating system user under which the files have been installed. A typical mistake is to install the executables in the `oracle` user's directory, but owned by `root`.

2. Check that the operating system user chosen as the owner of Oracle E-Business Suite owns all of the files in the `$APPL_TOP` directory.

3. Prevent remote login to the `oracle` (and `root`) accounts. Instead, require that legitimate users connect to their own accounts and `su` to the `oracle` account. Better yet, use `sudo` to restrict access to executables. Most operating systems now ship with `sudo`. Find more information about `sudo` at https://www.sudo.ws/. Another possibility is using Oracle Enterprise Manager with the Oracle E-Business Suite plug-in.

Cleaning Up File Permissions

Refer to the product installation documentation for the complete instructions on setting file permissions.

On UNIX systems:

1. Set the permissions on `$ORACLE_HOME/bin` to 0751 or less. Set all other directories in `$ORACLE_HOME` to 0750 or less. Note, this limits access to the Oracle user and its group (probably DBA).

2. Set file permissions for `listener.ora` and `sqlnet.ora` to 0600.

3. Set file permissions for `tnsnames.ora` to 0644.

4. Set file permissions for the database data files `*.dbf` to 0640.

5. Ensure that the owner, group and modes of the Oracle files created upon installation are set to allow minimum privilege. The following commands make this change. Note, the group and owner are for illustration only, the correct group and owner should be substituted.

   ```
   $chown -R <oracle> $ORACLE_HOME
   $chgrp -R <dba>    $ORACLE_HOM
   ```

6. Protect the `$ORACLE_HOME/rdbms/admin` directory including `catalog.sql`, `catproc.sql` and backup scripts.

7. On the application tier, ensure that the DBC files `$FND_SECURE/*.dbc` have mode 600.

8. Verify that set userid (SUID) and set group id (SGID) are not set on binaries. In general, Oracle recommends that the SUID and SGID bits to be removed from binaries shipped by Oracle.

   > **Warning:** If the concurrent manager runs on the database tier and is using the BEQ adapter to avoid TCP cost, the SUID and/or SGID bit must be set on the Oracle database executable in `$ORACLE_HOME/bin`. This may also apply for any third party products running on the database tier.

Locking Down Operating System Libraries and Programs

The database and applications require that the underlying operating system provide certain services.

1. **X Server**

   1. Oracle Installer requires access to the X server which in turn may require access to an X font server.

   2. Application tiers and web tiers do not require an X server.

3. A production database does not require access to an X server.

   This means that there is no requirement to install X on any of the Oracle E-Business Suite servers if a remote X Display can be provided during installation. Typically, the administrator's workstation can run the X Server and grant access to the Oracle E-Business Suite servers during installation.

2. **Printers**

   Applications may require access to printers - normally via the lpd interface on port 515/TCP. If possible, restrict access to the operating system users who absolutely need the printing facility from the shell.

3. **Email**

   Applications may require access to an SMTP Mail Transfer Agent (SMTP MTA) typically sendmail or qmail on port 25/TCP. This is required for outbound emails, typically notifications from the workflow system. If only outbound email is required in your environment, make the mail daemon listen on the localhost interface (127.0.0.1).

4. **Remote Access**

   Use Secure Shell (SSH + scp) to access application tier and database hosts. This replaces Telnet, rsh, rlogin, rcp and FTP, and it only requires one open port 22/TCP.

Although not required by Oracle E-Business Suite, the following services may provide operational convenience:

1. NTP (Network Time Protocol) - for synchronizing the clock on the UNIX hosts to provide accurate audit records and simplify troubleshooting.

2. CRON - for operating system cleanup and log file rotation

3. Monitoring agents - for monitoring operating system, database and application components for health and security

Network

To secure the network, limit access to services users need and make those services as secure as possible. Disabling unused services reduces securing and monitoring work.

Filtering IP Packets

IP packet filtering helps to prevent unwanted access. On the internet or a large network, use a firewall machine or router with firewalling capabilities.

A firewall machine sits between the internet and the intranet or the intranet and the internal servers. It provides a point of resistance by protecting inside systems from

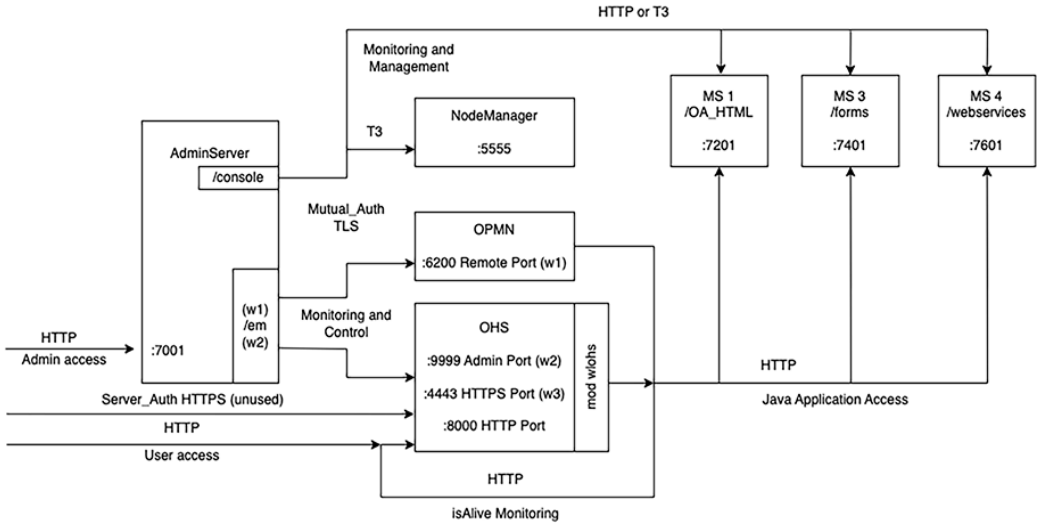
external users. A firewall machine can filter packets, or be a proxy server, or both. Firewalls may be software or hardware based. For software solutions, dedicate a machine to be the firewall. Do not assume that using Network Address Translation (NAT) substitutes for a firewall.

Filtering out unused services at the firewall or router level stops infiltration attempts earlier in the process. Unless running NFS between networks, block all RPC ports on the router. Better yet, implement a default OFF policy, open only those ports known to be required.

Ports to Open to Other Hosts on the LAN for a Single Primary Application Tier

If you have only one application tier, you may have the following network connections between processes on that host.

Example Network Connections Found in a Single Application Tier



This diagram illustrates all ports that need to be open to other hosts on the LAN or need to be open on the OS host firewall when a LAN is not set up. For example, port 8000 for OHS HTTP access, 4443 for OHS HTTPS access, and 7001 for WLS AdminServer access.

The network configuration for your application tier subnet should only allow access from the LAN to the web entry on OHS (HTTP or HTTPS) and optionally to the HTTP or HTTPS port on the WLS AdminServer.

If you do not have that level of network isolation, you will need to rely on the OS host firewall that by default denies all access except for specifically allowed traffic.

On the OS host firewall on the primary application tier, you must open the following listed ports to other hosts on the network.

- Port for the SSH client connection: 22/tcp

- One of the following HTTP or HTTPS ports for web entry:
  - 8000/tcp for OHS HTTP access
  - 4443/tcp for OHS HTTPS access
- Port for the WLS AdminServer connection (open this port if your administrators have workstations with static IP addresses): 7001/tcp

If you cannot list the specific host names or IP addresses for all your trusted hosts, then you can use alternative methods to allow access to the Oracle WebLogic Server Administration ports. See My Oracle Support Knowledge Document 2542826.1, *Alternative Methods to Allow Access to Oracle WebLogic Server Administration Console from Trusted Hosts for Oracle E-Business Suite Release 12.2*.

On a default Oracle Linux host (Oracle Linux 9, 8, or 7), the SSH port will typically be open by default, and you will need to provide access to the OHS web entry point (HTTP or HTTPS). To do so, replace `4443` with the actual port number used in your deployment.

```
# firewall-cmd --add-port 4443/tcp
# firewall-cmd --add-port 4443/tcp --permanent
```

To verify the open ports, run the following command. Services with well-known ports, such as sshd, are listed by service name.

```
# firewall-cmd --list-all
 public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3 enp0s8
  sources:
  services: ssh
  ports: 4443/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
```

Ports to Open on Application Tiers in a Multi Node Configuration

If you have more than one application tier, you will need a load balancer with LAN access and the FMW internal communication will need to cross the network between application tiers.

In this case, you must provide LAN access to the load balancer and implement host firewall rules that allow the internal FMW communication.

Therefore, the port must be open, but must be specific about what IP addresses are allowed to access the open port. To do this, ddefine "rich" rules rather than simply declaring the port "open to anyone" using the command `--add-port directive`.

An example of rules to add, assuming there are two application tiers, are as follows:

```
10.12.2.21  app01 primary-apptier
10.12.2.22  app02
```

Each application tier must allow network access to the following ports, but only to requests coming from one of the EBS application tiers.

- 6200/tcp OPMN Remote Port
- 9999/tcp OHS Admin Port
- 5555/tcp NodeManager

Access to the following WLS servers is restricted by the WLS connection filter, so they can be enabled without a "rich" rule.

- 7201/tcp OACORE Managed Server
- 7401/tcp Forms Managed Server
- 7601/tcp OAFM Managed Server

In addition, the OHS web entry (HTTP or HTTPS) must allow access from the load balancer IP addresses.

Still using Oracle Linux firewalld as the host firewall, examples of commands are as follows.

- Allow the AdminServer on the primary application tier access to OPMN Remote Port, OHS Admin Port, and NodeManager:

```
# firewall-cmd --add-rich-rule='rule family=ipv4 source address=10.
12.2.21/32 port port=6200 protocol=tcp  accept'
# firewall-cmd --add-rich-rule='rule family=ipv4 source address=10.
12.2.21/32 port port=9999 protocol=tcp  accept'
# firewall-cmd --add-rich-rule='rule family=ipv4 source address=10.
12.2.21/32 port port=5555 protocol=tcp  accept'
```

- Allow access to the WLS AdminServer and WLS managed servers (access restricted by WLS connection filter):

```
# firewall-cmd --add-port=7001/tcp
# firewall-cmd --add-port=7201/tcp
# firewall-cmd --add-port=7401/tcp
# firewall-cmd --add-port=7601/tcp
```

- Allow access to the OHS HTTP web entry from the load babancer (where the load balancer is the TLS termination point):

```
10.12.2.21  app01 primary-apptier
10.12.2.22  app02
10.2.2.19   lbr-int
```

```
# firewall-cmd --add-rich-rule='rule family=ipv4 source address=10.
2.2.19/32 port port=8000 protocol=tcp  accept'
```

The previously listed commands add the rules to the running version of firewalls. If testing shows that it is working as intended, repeat these commands on each of the

application tiers with the `--permanent` option added.

Create Access Control Lists

On the host, create access control lists in `/etc/ssh/sshd.conf` to limit which users can connect to the local machine. Turn off unused services in `/etc/inetd.conf`, or disable `inetd.conf` if no services require it.

Preventing Spoofing

To prevent host name spoofing, turn off source routing and filter packets originating outside the network that have source IP address from the inside network.

On the system side, only use fully qualified host names or IP addresses in system files.

For the production system consider enumerating all hosts that are part of the Oracle E-Business Suite instance in the hosts file on each system, this reduces the dependency on DNS for the core system.

Eliminating Telnet, RSH, and FTP Daemons

Enforce the use of SSH (Secure Shell). SSH provides encrypted traffic to prevent snooping. Telnet, rsh and FTP send the passwords in clear text and, for this reason, should not be used.

Verifying Network Configuration

Use scanning tools to find common security violations.

Monitoring For Attacks

Consider installing an Intrusion Detection System (IDS), For example, Snort is a capable and free IDS system.

Authentication

Good security requires secure accounts.

Configuring Accounts Securely

- Make sure all OS accounts have a non-guessable password. To ensure that the passwords are not guessable, use Crack or John the Ripper (password cracking tools) on a regular basis. Often, people use passwords associated with them: license plate numbers, children's names, or a hobby. A password tester may check for these. In addition, change passwords from time to time.

- Automatically disable accounts after several failed login attempts.

Limiting Root Access

- The fewer people with root access, the easier it is to track changes.
- The root password must be a strong, non-guessable password. In addition, change the root password every three (3) months and whenever an administrator leaves company. Always logout of root shells; never leave root shells unattended.
- Limit root to console login, only (specified in `/etc/security`).
- Root, and only root, should have UID 0.
- Check root '.*' files for security holes. The root '.*' files SHOULD have 700 or 600 permissions. The minimal umask for root is 022 (rwxr-xr-x). A umask of 077 (rwx------) is best, but often not practical.
- To avoid Trojan horse programs, always use full path names including aliases. Root should never have "." in path. Never allow non-root write access to any directories in root's path.
- If possible, do not create root's temporary files in publicly writable directories.

Managing User Accounts

Do not share user accounts. Remove or disable user accounts upon termination. Disable login for well-known accounts that do not need direct login access (bin, daemon, sys, uucp, lp, adm). Require strong passwords and, in some cases, a restricted shell.

Authorization

Securing NFS

Only run NFS as needed. When creating the `/etc/exports` file, use limited access flags when possible (such as readonly or nosuid).

Securing Operating System Devices

Device files `/dev/null`, `/dev/tty`, and `/dev/console` should be world writable but never executable. Most other device files should be unreadable and unwritable by regular users.

Securing Executables

Always get programs from a known source. Use a checksum to verify they have not been altered.

Securing File Access

Create minimal writable file systems (esp. system files/directories). Limit user file writes to their own directories and `/tmp`. Add directories for specific groups. Limit important file access to authorized personnel. Use setuid/setgid only where absolutely necessary.

Maintenance

Good security practice does not end after installation. Continuous maintenance tasks include:

- Regularly run the Security Check Scripts on your production instance to ensure that it is, and continues to be, in compliance with the recommendations in this document. Reference My Oracle Support Knowledge Document 2069190.1, *Security Configuration and Auditing Scripts for Oracle E-Business Suite*, for more information on how to run the Security Check Scripts.

- Install the latest software patches and stay current on the latest Critical Patch Updates (CPUs).

- Install latest operating system patches.

- Verify user accounts - delete or lock accounts no longer required.

- Run security software and review output.

- Keep up to date on security issues by subscribing to security mailing lists, reading security news groups and following the latest security procedures.

- Test the system with Application Fuzzing tools, network security tools, and password crackers. See Appendix A: Running Web-Scanning Tools, page A-1 for information about false positives when running these tools.

- Install Tripwire to detect changes to files.

- Monitor log files including btmp, wtmp, syslog, sulog, etc. Consider setting up automatic email or paging to warn system administrators of any suspicious behavior. Also check the snort log.

13

Secure Configuration Console

Overview

The Secure Configuration Console automates the security configuration process, consolidates everything under one user interface, and creates a single checkpoint entry into the system. It ensures that high priority security configuration problems are reviewed, understood, and remediated, ensuring a secure Oracle E-Business Suite environment.

After you upgrade to the latest ATG_PF Release Update Pack, your system will be "locked down" until a local system administrator resolves or acknowledges the recommended security configurations in the Secure Configuration Console.

To access this console, a user must have a responsibility that includes the Applications System (OAM_APP_SYSTEM) function privilege, such as the seeded System Administration or System Administrator responsibilities, and must be registered as a local user with Oracle E-Business Suite. The administrator must log in to Oracle E-Business Suite using the local login page (`http(s)://[host]:[port]/OA_HTML/AppsLocalLogin.jsp`) to navigate to the console and unlock the system. If a user with local system administrator privileges is not available, you can access the Secure Configuration Console through a command line utility (described later in this section).

Once the system is unlocked for normal usage, the Secure Configuration Console is still available for administrators under the Functional Administrator responsibility.

Feature Overview

The Secure Configuration Console provides:

- **Restricted login**
  - Login into the system is completely restricted in "Locked Down" mode.

    - Access to the system is provided by performing the recommended secure configuration or acknowledging secure configuration recommendations.

- **A single view of the system's security health**
    - Consolidated view of all security recommendations for different layers such as network, database, and application.
    - View detailed descriptions of security configurations.
    - Review the current status, severity level, and type (autofixable/manual) of security configurations.
    - Provides complete picture of security health of the system.

- **Secure configuration management**
    - Analyzes the current state of the configuration.
    - Resolves on-the-fly autofixable secure configurations as per Oracle E-Business Suite recommendations.
    - Mute or unmute the configurations as per administrator choice.

Benefits

Automating the high priority security configuration process provides the following benefits:

- Security threats are prevented by ensuring secured configuration of the system.
- Security vulnerabilities can be resolved as entry into the system is prevented until it is reviewed for security configuration.
- All high-priority Oracle E-Business Suite secure configurations are available to review in one place.
- Manual configurations, which are cumbersome and error-prone, are minimized.
- Management of configurations is quick and easy.

Using the Secure Configuration Console

There are two methods to access the Secure Configuration Console home page.

- Using the Functional Administrator responsibility:

On the Oracle E-Business Suite home page, select the **Functional Administrator** responsibility in the Navigator pane. Then, on the Functional Administrator page, select the **Configuration Manager** tab.

- Using the OAM Security Dashboard:

  On the Oracle E-Business Suite home page, select **System Administrator** in the Navigator pane. Then select **Oracle Applications Manager**, then **OAM Security Dashboard**. On the dashboard, under the Configuration Management section is a link to the Secure Configuration Console.

The Secure Configuration Console bases its recommendations on recommended security guidelines. They are listed in more detail in the following section, Checked Security Guidelines, page 13-3.

You can search for a recommendation by guideline, code, configuration type, status, or level of severity in the Search section or by perusing through the table itself.

The following actions are available:

- **Check** - Discover the status of selected guideline check before configuring
- **Fix** - Resolve the status of a selected failed guideline check
- **Suppress** - Mute guidelines that are not relevant to your system
- **Unsuppress** - Unmute previously suppressed guidelines
- **Check All** - Discover the status of all unsuppressed guidelines

Checked Security Guidelines

Updates to the checks performed by the Secure Configuration Console are delivered with Oracle E-Business Suite ATG Release Updates (RUPs) or Critical Patch Updates (CPUs). We highly recommend that you apply the latest ATG RUP or latest CPU to ensure that all recommended secure configuration checks are available for your environment. See the following My Oracle Support knowledge documents for more information:

- Document 1583092.1 - *E-Business Suite RUP, AD and TXK RUP Information, Release 12.2* [http://support.oracle.com/rs?type=doc&id=1583092.1]
- Document 2484000.1 - *Identifying the Latest Critical Patch Update for Oracle E-Business Suite Release 12.2* [http://support.oracle.com/rs?type=doc&id=2484000.1]

If you are not running the latest release of the Secure Configuration Console, see Obsolete Secure Configuration Console Checks for Security Guidelines, page H-2 for obsolete checks which may still be running in your environment.

If any of the guidelines listed in the following table fail the secure configuration check,

you can either fix or suppress the failure. For a secure environment, Oracle recommends that you address all failures that are applicable to your environment.

The Secure Configuration Console currently checks the following high priority secure configuration guidelines:

Security Guidelines Checked by the Secure Configuration Console

Security Guideline	Description	Code	Severity	References
Allowed Resources Configuration (Release 12.2.7 and later)	Check whether the Allowed Resources feature is enabled.	FND_JSP_UNREST_ACC	1	• Allowed Resources, page 4-82
Application Users Default Password	Check whether all application users' default passwords have been changed to non-default values.	FND_APPS_DEF_PSWD	1	• Changing Passwords for Seeded Application User Accounts, page 10-19
Attachment File Type Profiles	Check whether attachment upload profiles are available and set correctly in the system.	FND_MISS_ATT_PROF	1	• Securing Attachments, page 10-2
Clickjacking Protection (Release 12.2.7 and later)	Check whether clickjacking protection is configured.	CLICKJACK_PROTECTION	1	• Using Certified HTTP Security Headers, page 10-9

Security Guideline	Description	Code	Severity	References
Critical Security Profile Values	Check whether critical security profile values are set correctly at all levels (for example: site, responsibility, user).	FND_PROF_ERRORS	1	• Setting Other Security-Related Profile Options, page 10-30
Database Users Default Passwords	Check whether all database users default passwords have been changed.	FND_DB_DEF_PSWD	1	• Changing Default Installation Passwords, page 8-2 • My Oracle Support Knowledge Document 361482.1, *Frequently Asked Questions about Oracle Default Password Scanner*
Diagnostic Web Pages Protected (Release 12.2.7 and later)	Check whether diagnostic web page protection is configured.	DIAG_WEB_PAGE_PROTEC	1	• Protecting Administrative Pages, page 9-2

Security Guideline	Description	Code	Severity	References
Forms Blocking of Bad Characters	Check whether the Forms blocking of "bad" characters on the web server is active.	FND_FORMS_BLOCK_CHR	1	Log a Service Request (SR) in My Oracle Support. Reference the Secure Configuration Console and the failed Forms Blocking of Bad Characters check.
Missing Server Security Profile	Check whether site level security profiles are available in the system.	FND_MISS_PROF	1	Log a Service Request (SR) in My Oracle Support. Reference the Secure Configuration Console and the failed Missing Server Security Profile check.
ModSecurity Configuration	Check whether ModSecurity on the web server is active.	FND_MOD_SEC	1	Log a Service Request (SR) in My Oracle Support. Reference the Secure Configuration Console and the failed ModSecurity Configuration check.

Security Guideline	Description	Code	Severity	References
Oracle E-Business Suite CPU Patch Level Check	Check whether the Oracle E-Business Suite Critical Patch Update patch in the system is greater or equal to the configured value of the FND_SEC_MIN_CPU_PATCH_LEVEL (FND: Minimum CPU Patch Level) profile option.	FND_MIN_CPU_LEVEL	1	• My Oracle Support Knowledge Document 2484000.1, *Identifying the Latest Critical Patch Update for Oracle E-Business Suite Release 12*

Security Guideline	Description	Code	Severity	References
PUBLIC Privileges (Release 12.2.7 and later)	Check whether the PUBLIC role privileges are restricted.	FND_APPS_IND_PUBLIC	1	This checks whether unnecessary privileges to Oracle E-Business Suite object have been granted to the Oracle Database PUBLIC role. You should revoke unnecessary privileges from the PUBLIC role. Oracle E-Business Suite database objects should not have privileges granted to the PUBLIC role. Any privileges granted to the PUBLIC role from Oracle E-Business Suite objects should be revoked. Certain privileges, such as the ability to create indexes, can be leveraged for privilege escalation in the database and should be removed.

Security Guideline	Description	Code	Severity	References
WebLogic Server Default Password (Release 12.2.9 and later)	Check whether WebLogic Server default password has been changed to a non-default value.	FND_WLS_DEF_PSWD	1	• Change Password for WebLogic Server Admin User, page 10-29
Workflow Email Link Login (Release 12.2.7 and later)	Check whether Oracle Workflow generated emails that reference URLs in Oracle E-Business Suite require additional user authentication (login).	WF_EMAIL_LOGIN	1	• Setting Workflow Notification Mailer SEND_ACCESS_KEY to N, page 10-1
APPLSYSPUB Privileges	Check whether APPLSYSPUB privileges are properly restricted.	FND_APPLSYSPUB	2	• Revoking Unnecessary Grants Given to APPLSYSPUB, page 8-5
Activate Server Security	Check whether server security (Secure Flag in DBC file) is enabled.	FND_SERVER_SEC	2	• Activating Server Security, page 10-27
Allowed Redirects	Check whether the Allowed Redirects feature is enabled.	FND_UNREST_REDIR	2	• Allowed Redirects, page 4-101 • Configuring Allowed Redirects, page 9-1

Security Guideline	Description	Code	Severity	References
Auditing Profile Values	Check whether the FND: Debug Log and Sign-on Audit profile values are set correctly.	FND_AUDIT_PROF	2	• "Using Oracle Application Object Library Profile Options to Configure Logging," *Oracle E-Business Suite Maintenance Guide* • "Page Access Tracking and Sign-On Audit," *Oracle E-Business Suite Maintenance Guide* • Sign-On Audit, page 16-3
Cookie Domain Scoping Configuration	Check whether Cookie Domain Scoping is configured.	FND_COOKIE_DOM	2	• Cookie Domain Scoping, page 4-79 • Using Certified HTTP Security Headers, page 10-9

Security Guideline	Description	Code	Severity	References
Database Network Access Control List (Release 12.2.10 and later)	Check if Database Network Access Control List has been enabled.	SEC_DB_NETWORK_ACL	2	• My Oracle Support Knowledge Document 2500511.1, *Implementing Database Network Access Control Lists*

Security Guideline	Description	Code	Severity	References
Database Parameters (init*.ora) (Release 12.2.7 and later)	Check whether secure configuration recommended database initialization parameters have been set.	FND_INIT_ORA	2	• Removing Operating System Trusted Remote Logon, page 8-2 • Removing Operating System Trusted Remote Roles, page 8-4 • Restricting Access to SQL Trace Files, page 8-4 • Limiting File System Access Within PL/SQL, page 8-5 • Limiting Dictionary Access, page 8-5
Database Password Profiles (Release 12.2.7 and later)	Check if secure configuration recommended database profiles have been created in the Oracle E-Business Suite database.	SEC_DB_PSWD_PROF	2	• Implementing Two Profiles for Password Management, page 8-3

Security Guideline	Description	Code	Severity	References
FND Generic File Manager (FNDGFM) Authorization Configuration	Check whether the system is compliant with the recommended configuration for FND Generic File Manager (FNDGFM) authorization.	FNDGFM_AUTH_CONFIG	2	• My Oracle Support Knowledge Document 1357849.1, *Security Configuration Mechanisms in the Attachments Feature in Oracle E-Business Suite*
HTTPS Configuration	Check whether HTTPS is enabled.	FND_SSL_ENABLED	2	• Using TLS to Encrypt Oracle E-Business Suite Connections, page 10-18
Hashed Passwords	Check whether application user passwords have been migrated to hashed passwords.	FND_PSWD_HASH	2	• Switching to Hashed Passwords, page 10-24
iRecruitment File Upload Profile (Release 12.2.7 and later)	Check whether the iRecruitment File Upload profile (IRC: XSS Filter) value is set.	IREC_FILE_UPLOAD	2	• *Oracle iRecruitment Implementation and User Guide*, Release 12.2

Security Guideline	Description	Code	Severity	References
Unused Allowed Resources	Check whether unused resources are denied.	SEC_UNUSED_ RESOURCES	2	It is recommended to deny access to resources which have not been used in a year. These can be viewed in the Management by Resource tab on the Allowed Resources user interface. For more information, see Allowed Resources, page 4-82.
Workflow Admin Access (Release 12.2.7 and later)	Check whether Oracle Workflow Admin access is restricted.	WF_ADMIN_N OT_PUBLIC	2	• Ensuring You Know Who is a Workflow Admin, page 10-1

Updates to the checks performed by the Secure Configuration Console are delivered with Oracle E-Business Suite ATG Release Updates (RUPs). We highly recommend that you apply the latest ATG RUP to ensure that all recommended secure configuration checks are available for your environment. See My Oracle Support Knowledge Document 1583092.1, *E-Business Suite RUP, AD and TXK RUP Information, Release 12.2*, for more information.

If any of the guidelines listed in the previous table fail the secure configuration check, you can either fix or suppress the failure. For a secure environment, Oracle recommends that you address all failures that are applicable to your environment.

Navigating Through the Secure Configuration Console

On the main screen of the console are four predefined filtered criteria in tiles added in Oracle E-Business Suite Release 12.2.10. Click on each tile to view the filtered guidelines in the table displayed.

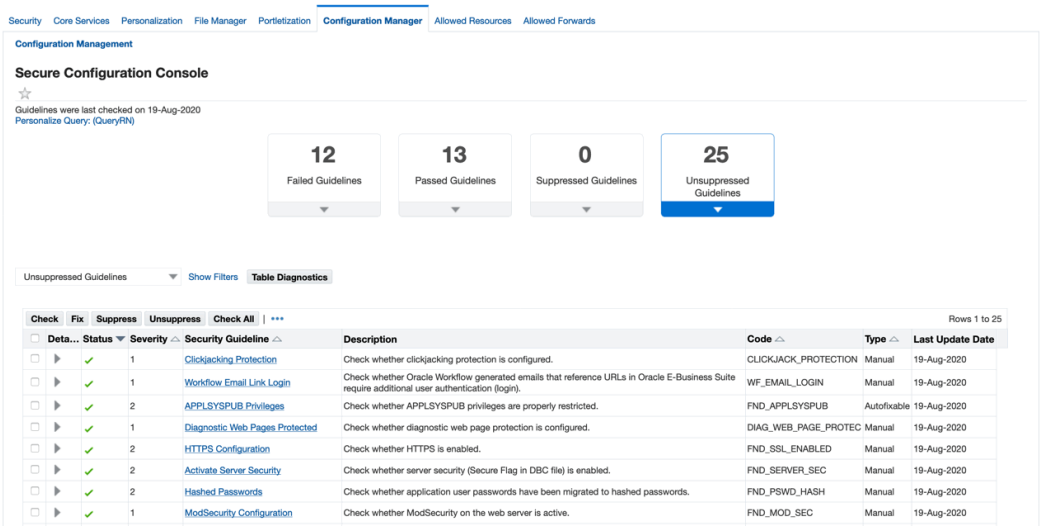
- **Failed Guidelines** - By default, this filter provides all Severity 1 and Severity 2 level

failures, but not guideline checks that have been suppressed.

- **Passed Guidelines** - This shows all guideline checks that have passed, but not those that have been suppressed.
- **Suppressed Guidelines** - This shows all guideline checks that have been suppressed (or muted).
- **Unsuppressed Guidelines** - This shows all guidelines that have not been suppressed. These are the security guidelines that are being checked.

The "Guidelines were last checked on" date above the left most tile is the date in which the security guidelines were checked against using the Secure Configuration Console.

Secure Configuration Console Main Page



You can further refine each tile's criteria by utilizing the Saved Search drop-down. The drop-down allows you to add additional filter criteria which displays in the Filter section on the left, where you can save your search for future use.

In the table on the main console page, click **Check** to compute the status of all configurations on your system against the selected guidelines. Click **Check All** to select and check all guidelines.

Once the status is computed, the guideline will display as either as Pass or Fail (green check mark or red X, respectively) in the Status column.

Click on the arrow in the Details column for more information as to why a certain configuration passed, failed, or produced an error during the configuration check.

Secure Configuration Console Checked Guidelines Table

Check | Fix | Suppress | Unsuppress | Check All | ••• Rows 1 to 25

Deta...	Status	Severity	Security Guideline	Description	Code	Type	Last Update Date
	✓	1	Clickjacking Protection	Check whether clickjacking protection is configured.	CLICKJACK_PROTECTION	Manual	19-Aug-2020
Passed. OK: X-Frame-Options is active onhttps://rws3270880.us.oracle.com:4443 Detailed information can be obtained from /u01/R122_EBS/fs2/inst/apps/atqax07c_rws3270880/logs/adminsecuritycfg_4930687.log							
	✓	1	Workflow Email Link Login	Check whether Oracle Workflow generated emails that reference URLs in Oracle E-Business Suite require additional user authentication (login).	WF_EMAIL_LOGIN	Manual	19-Aug-2020
	✓	2	APPLSYSPUB Privileges	Check whether APPLSYSPUB privileges are properly restricted.	FND_APPLSYSPUB	Autofixable	19-Aug-2020
	✓	1	Diagnostic Web Pages Protected	Check whether diagnostic web page protection is configured.	DIAG_WEB_PAGE_PROTEC	Manual	19-Aug-2020
	✓	2	HTTPS Configuration	Check whether HTTPS is enabled.	FND_SSL_ENABLED	Manual	19-Aug-2020
	✓	2	Activate Server Security	Check whether server security (Secure Flag in DBC file) is enabled.	FND_SERVER_SEC	Manual	19-Aug-2020

To automatically remediate failed configuration checks, select guideline checks with a Failed status and of the type Autofixable and click **Fix** located at the top of the table to resolve the reported issues.

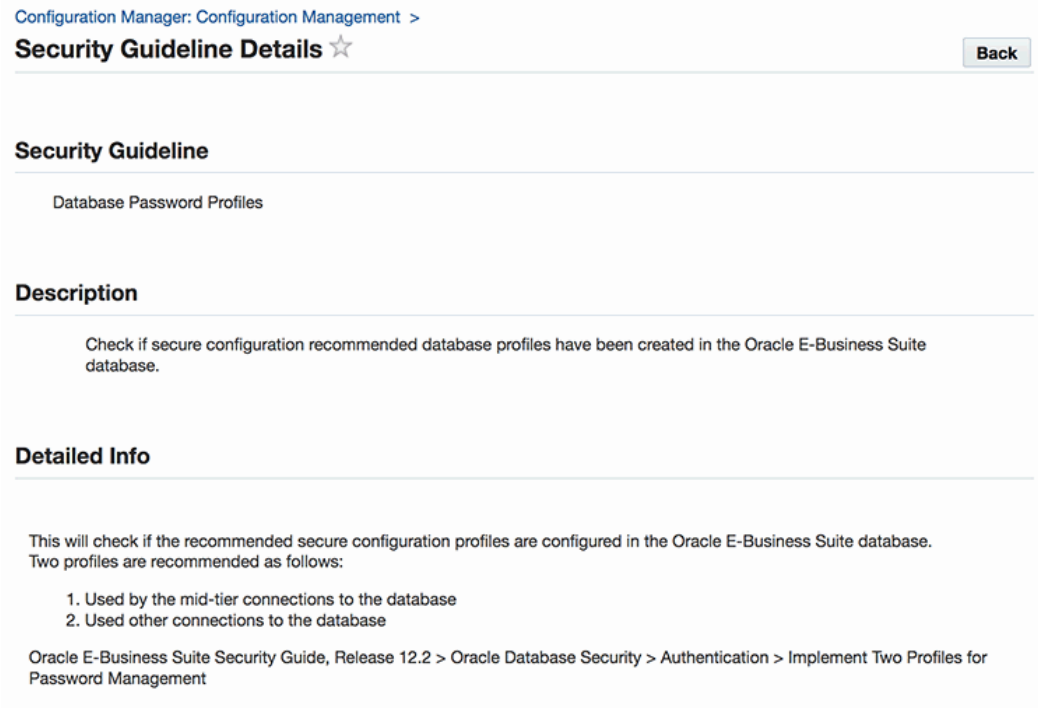
Click **Suppress** to mute selected guideline checks that are NOT applicable to your system. Suppressed guidelines will no longer be displayed, nor will they require further review in the console when deselecting the Muted Security Configuration checkbox.

Click **Unsuppress** to unmute the previously muted guideline checks.

Each security guideline is a link, which when clicked, opens a new page with a detailed description of the configuration requirement.

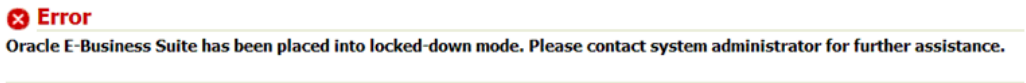
If the configuration requirement involves a manual fix, more information on the necessary manual steps can be found by clicking the link. For example, when clicking the "Database Password Profiles" link, the Security Guideline Details page is displayed, providing the security guideline description and detailed information about the check.

Security Guideline Details Page



As mentioned previously, until the recommended security configurations have been implemented or acknowledged by a local system administrator, the Secure Configuration Console will prevent entry into the system. Until then, users will see an error message when trying to log in which says: "Oracle E-Business Suite has been placed into locked-down mode. Please contact system administrator for further assistance."

Locked-Down Mode Error Message



When an Oracle E-Business Suite instance has been placed into locked-down mode, as soon as a user with system administrator privileges logs in the Secure Configuration Console will appear.

At this point, the system administrator should resolve or address any failed security guideline checks. When ready to unlock the instance, the system administrator should select either of the following options prior to clicking **Proceed**:

- I am done with the security configurations.
- Ignore the security configurations.

Once you click **Proceed**, the Oracle E-Business Suite instance is unlocked.

Command Line Utility

If a user with local system administrator privileges is not available, you can access the Secure Configuration Console by using the `AdminSecurityCfg` utility.

This utility is provided for the following tasks:

- To take the system out of locked down mode.
- To compute the status of a certain configuration or all configurations.
- To configure a certain configuration or all configurations of type Autofixable.
- To view the status of a certain configuration or all configurations.

To use the `AdminSecurityCfg` utility, use the following syntax which will then will prompt you for your `<APPS Username>` and `<APPS password>`. Note that all parameters can, if desired, be entered on the same command line; they are shown here on different lines (using the UNIX '\' continuation character) for clarity.

```
java oracle.apps.fnd.security.AdminSecurityCfg \
<-check|-fix|-status|-lock|-unlock> \
DBC=<DBC File Path> \
[CODES=<code1>,<code2>,<code3>...]
```

Where:

`-check` - Runs the utility in check mode. You can specify the configurations to check by adding `[CODES=<code1>,<code2>,<code3>...]` to the command. These correspond to the security guideline codes found in Security Guidelines, page 13-4.

For example: `java oracle.apps.fnd.security.AdminSecurityCfg -check DBC=<DBC File Path> CODES=FND_DB_DEF_PSWD,FND_PROF_ERRORS`

If you do not specify a `CODES` attribute, then the utility will check all configurations.

`-fix` - Runs the utility in fix mode. You can specify the configurations to fix by adding `[CODES=<code1>,<code2>,<code3>...]` to the command.

For example: `java oracle.apps.fnd.security.AdminSecurityCfg -fix DBC=<DBC File Path> CODES=FND_UNREST_REDIR,FND_AUDIT_PROF`

If you do not specify a `CODES` attribute, then the utility will fix all configurations of type Autofixable.

`-status` - Determines the status of all configurations. Specifying the `CODES` attribute is not necessary for this mode.

`-lock` - Places the system in locked down mode.

`-unlock` - Takes the system out of locked down mode.

Part 3

Guidelines for Auditing and Logging

14

Introduction to Guidelines for Auditing and Logging

About Auditing and Logging

Satisfying compliance regulations and reducing the risk of security breaches are among the top security challenges businesses face today. Examination of numerous security incidents has shown that timely examination of audit data could have helped detect unauthorized activity early and reduced the resulting impact. Well-known regulations, such as the Sarbanes-Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPAA), combined with industry driven initiatives, such as the Payment Card Industry Data Security Standard (PCI-DSS), and the proliferation of Breach Notification laws, have resulted in information protection becoming a top-level issue for the enterprise. As security threats become more sophisticated, monitoring is becoming an increasingly important component of the defense-in-depth architecture.

Unauthorized access, use, or disclosure of sensitive and critical information can seriously impact both individuals, by contributing to identity theft, and the organization, by reducing public trust in the organization. It is not enough to simply secure such data, but companies must also provide auditing as a means of ensuring compliance.

Oracle E-Business Suite and its associated technology stack provide a variety of auditing mechanisms to address different requirements. This document is intended to introduce and describe the various auditing mechanisms available, what tasks they should be leveraged for, and recommendations for how to configure them in the context of Oracle E-Business Suite.

Why Audit?

There are many different reasons for configuring an Oracle E-Business Suite environment for auditing and logging. The most common reasons that administrators are required to configure auditing and logging include the following:

- Monitor system and database activity
- Detect suspicious activity and attacks
- Investigate incidents after an attack
- Monitor for compliance reasons, including SOX, HIPPA, PCI-DSS
- Perform business process monitoring to implement business controls
- Monitor performance of the environment

Similarly, there are a variety of roles that may be interested in auditing different aspects of Oracle E-Business Suite:

- External/internal audit teams
- Security teams
- Technical system administrators (Apps DBAs/UNIX DBAs)
- Functional system administrators and users

While the mechanisms described in this document will be useful for any of the reasons and roles mentioned above, we will be focusing on monitoring the Oracle E-Business Suite application and technology stack to monitor current usage, how to detect attacks and suspicious activity, and auditing and logging configuration that will allow for a more comprehensive incident investigation after an attack.

15

Auditing and Logging Features in Oracle E-Business Suite

Overview of Features

Oracle E-Business Suite, the Oracle E-Business Suite technology stack, and optional Oracle Technology integrations provide various auditing and logging capabilities. Deciding which one to use and how to use it will depend on what you're trying to achieve.

The auditing and logging features described in this chapter can assist with analyzing the following:

- Recent and current activity
- Historical activity
- Unexpected events

Recent and Current Activity

Recent and Current Activity encompasses information about what is happening in the system currently, or what the last activity was performed on particular record or done by a particular session. This includes the following Oracle E-Business Suite features:

- Data changes tracked with row who columns - Records information about who and when each record was created and last updated
- Sign-on Audit and Session Audit information - Records information about each user session, as well as the last activity performed on that session
- Database connection tagging - Records Oracle E-Business Suite session information in v$session

Historical Activity

Historical Activity features capture similar information to the information described in the previous section, but retain historical data about what has been changed. This is sometimes switched off by default in the Oracle E-Business Suite environment and can be switched on for targeted areas of Oracle E-Business Suite. Auditing mechanisms that fall into this category include the following features:

Oracle E-Business Suite

- Page Access Tracking - Captures historical information about what users were doing in the system and what the performance was, as well as allowing to what a specific user and sessions were accessing

- Oracle E-Business Suite Audit Trail - Uses database triggers and shadow tables to record historical data about changes to specific tables (not to be confused with the similar Database Audit Trail feature). It provides a straightforward user interface for defining which tables you wish to audit in this manner. Because the auditing tables reside in the Oracle E-Business Suite database, it's easier to report on them, but this mechanism does not provide the performance and integrity of the audit records that can be achieved with Oracle Database Auditing discussed in the next section.

- Proxy User Auditing - Tracks the usage of the Oracle E-Business Suite Proxy User feature and provides reports which can be used to audit the use of this feature. This auditing is on by default.

Oracle E-Business Suite Applications Technology Stack

- OHS Apache Access Logs - Tracks all HTTP GET requests that come into Oracle E-Business Suite, along with their parameters. This auditing is on by default.

- Database Listener Logs - Tracks database listener commands and connections to the database.

- Database Auditing - Monitors and records configured database actions. It can be used to track table changes, in a manner similar to the Audit Trail feature discussed above.

- Fine-Grained Auditing - Allows detailed conditions to trigger auditing of data access based on content

Unexpected Events

Certain areas of Oracle E-Business Suite in the underlying technology stack report on unexpected errors. These unexpected events can include security related events.

Oracle E-Business Suite Applications

- Unsuccessful Login Attempts - Captures information about unsuccessful login attempts
- Debug Logging (Unexpected Logging) - Captures debug information at a variety of levels. At the default level of Unexpected, Oracle E-Business Suite captures information about unexpected events.

Oracle E-Business Suite Applications Technology Stack

- OHS Apache Error Logs - Captures unexpected events that occur at the Oracle HTTP Server level. This includes potential attacks that have been blocked by Mod Security.
- Oracle Database Listener Log - Captures unexpected connection errors
- Oracle Database Alert Log - Captures unexpected database errors

Oracle E-Business Suite Auditing Scripts

Throughout this document, we will be referring to SQL scripts that can be used as follows:

- Configure auditing for the database
- Query various auditing tables described in this guide
- Validate that your auditing configuration meets the recommendations described in this guide

> **Note:** Many of the scripts that are provided serve as examples only. The intent is that administrators and auditors can leverage and customize these scripts to meet their specific needs. Scripts mentioned here, as well as other security related scripts, can be found as an attachment to My Oracle Support Knowledge Document 2069190.1, *Security Configuration and Auditing Scripts for Oracle E-Business Suite*.

16

Using Oracle E-Business Suite Application Auditing and Logging Features

Introduction

This chapter describes how to configure and use Oracle E-Business Suite audit and logging features. It provides an explanation of the features available, configuration steps and best practices for auditing. It also suggests which common application objects (such as foundation objects, users, and responsibilities) to audit.

Unsuccessful Login Attempts

Oracle E-Business Suite automatically stores unsuccessful local logon attempts in APPLSYS.FND_UNSUCCESSFUL_LOGINS. This functionality cannot be disabled. Only names of valid users in FND_USERS will be recorded. Unsuccessful logins are not recorded by Oracle E-Business Suite if you have integrated with Oracle Access Manager for single sign-on.

The following options are available for reviewing the information recorded by Unsuccessful Login Attempts:

- Use the `UnsuccessfulLogins.sql` script provided My Oracle Support Knowledge Document 2069190.1, *Security Configuration and Auditing Scripts for Oracle E-Business Suite*.
- Run the Signon Audit Unsuccessful Logins report.

Data Changes Tracked with Who Columns

Oracle E-Business Suite tracks data changes automatically within a record. For most Oracle E-Business Suite tables, database rows are updated with the creation and last update information. The system stores this information in the following columns

known as *Who Columns*:

Who Column Descriptions

Who Column Name	Description
`CREATION_DATE`	Date and Time row was created
`CREATED_BY`	Oracle Applications user ID from FND_USER
`LAST_UPDATE_LOGIN`	Login ID from FND_LOGINS
`LAST_UPDATE_DATE`	Date and Time row as last updated
`LAST_UPDATED_BY`	Oracle Applications user ID from FND_USERS

Join with FND_USERS table to identify the application user tracked in the audit record. Or join with FND_LOGINS for the associated login record. Note that only the last update to record is saved.

For example, if you want to see the Who column information of changes to Profile Values for the last ten days, you could use the following SQL:

```
select p.profile_option_name "Internal name",
        fpv.PROFILE_OPTION_VALUE value,
        cr.user_name "Created",
        to_char(fpv.creation_date,'DD-MON-RRRR HH24:MI:SS') "Creation
Date",
        upd.user_name "Updated",
        to_char(fpv.last_update_date,'DD-MON-RRRR HH24:MI:SS') "Update
Date",
        to_char(ll.start_time,'DD-MON-RRRR HH:MI:SS') "Login Time"
from fnd_profile_options p,
         fnd_profile_option_values fpv,
     fnd_user upd,
     fnd_user cr,
     fnd_logins ll
where p.profile_option_id = fpv.profile_option_id (+)
and fpv.last_updated_by=upd.user_id (+)
and fpv.created_by=cr.user_id (+)
and fpv.last_update_login=ll.login_id (+)
and fpv.last_update_date > sysdate-10;
```

Sign-On Audit

Oracle E-Business Suite provides a Sign-On Audit feature that allows you to:

- Track what your users are doing, from where, and when they do it.
- Choose who to audit and what type of information to audit.
- View quickly online what your users are doing.
- Check the security of your application.

> **Note:** Most of the Sign-On Audit reports are specific to the Oracle Forms interfaces. Information about Oracle Application Framework (OAF) and Oracle CRM Technology Foundation (JTF) session information can be found through the SQL queries and Page Access Tracking described in the following sections.

With Sign-On Audit, you can record user names, terminals, and the dates and times your Oracle Forms users access Oracle E-Business Suite. Sign-On Audit can also track

the responsibilities and forms your users use, as well as the concurrent processes they run. You also have the ability to monitor user activity and submit reports for detailed audit information. Use the Submit Reports form to submit Sign-On Audit Reports that give you detailed audit information.

Sign-On Audit Reports give you historical, detailed information on what your Forms users do in your application. You can give search criteria to narrow your search for information. You can also sort your Sign-On Audit information to create easy-to-read reports. You will only generate reports for users that are being audited by Sign-On Audit.

Enabling Sign-On Audit

You use the Sign-On:Audit Level user profile option to control who Sign-On Audit tracks and the level at which they are audited. Sign-On Audit lets you choose who to audit and what type of user information to track. You can selectively determine what audit information you need to match your organization's needs.

Use the System Profile Values form to enable Sign-On Audit. Choose the scope of your audit and who to audit by setting the user profile level at the user, responsibility, application, or site profile levels.

> **Note:** Users cannot see or change this profile option.

After you set or change audit levels, the new audit levels for a user take effect the next time the user signs onto Oracle E-Business Suite.

Select Audit Levels

The Sign-On:Audit Level profile provides varying levels of Oracle E-Business Suite sign-on information. Based on the audit level chosen, Sign-On audit records user names, dates, and times of system access, as well as users' terminals, Forms, and responsibilities.

Four audit levels provide increasing levels of monitoring: *None*, *User*, *Responsibility*, and *Forms*.

All user logins, responsibility selections, and form accesses will be logged to APPLSYS. FND_LOGINS, APPLSYS.FND_LOGIN_RESPONSIBILITIES, and APPLSYS. FND_LOGIN_RESP_FORMS, respectively.

Auditing Level None Tracks:

- No activities by any users who sign on to Oracle E-Business Suite

Auditing at the User Level Tracks:

- Who signs on to your system
- The times users log on and off
- The terminals in use
- Client IP addresses (starting with Release 12.2.10 and later or R12.ATG_PF.C.Delta.9)

Auditing at the Responsibility Level Performs the User Level Audit Functions and Also Tracks:

- The responsibilities users choose, including both responsibilities for Forms-based applications and responsibilities for HTML-based applications built with Oracle Application Framework or Oracle CRM Technology Foundation
- How much time users spend using each responsibility

> **Note:** For HTML-based applications, auditing tracks the time users spend in a responsibility context. Note that the responsibility context does not change when a user navigates back to the Oracle E-Business Suite home page from an HTML-based application page. The context changes only when the user goes to a page with a different responsibility.

Auditing at the Form Level is Default, Performs the Responsibility and User Level Audit Functions and Also Tracks:

- The forms users choose
- How long users spend using each form

It is recommended to set Sign-On:Audit Level to Form so the application will track every log on to the application, every responsibility used by the users, and every form opened by the users. This profile option tracks Forms usage only.

Audit Levels and System Overhead

In planning your organization's Sign-On Audit implementation, you should consider the additional system overhead required to monitor and audit your users as they access Oracle E-Business Suite. The more users you audit, and the higher the level of auditing, the greater the system overhead such as processing costs and disk space. You should balance your organization's auditing needs with the resources available, obtaining additional resources if the existing ones are insufficient to support the required auditing

activities as well as the actual workload.

Example - Audit Users, Responsibilities, and Forms

An example implementation of Sign-On Audit would be to audit all of your users' sign-ons, the responsibilities they select, and the forms they access.

To accomplish this, you would set Sign-On:Audit Level to:

- Form audit
- At the site profile level

Example - Audit a Specific Responsibility, Except for One User

Another example of using Sign-On Audit is for an organization to audit all users of the Personnel Manager responsibility, except for MJONES.

In this example, you do not need to audit the forms the user accesses, or the responsibilities they select.

To set up this implementation, set Sign-On:Audit Level to:

- User audit
- At the Responsibility profile level for the Personnel Manager responsibility

You also set Sign-On:Audit Level to:

- None
- At the User profile level for the application user MJONES

Notification Upon Unsuccessful Logins

Sign-On Audit can track user logins and provide users with a warning message if anyone has made an unsuccessful attempt to sign on with their application user name since their last sign-on. This warning message appears after a user signs on.

You or your users can activate this feature using the Personal Profile Values form by setting the Sign-On:Notification user profile option to Yes.

You do not have to audit the user with Sign-On Audit to use this notification feature.

Monitor Users

Monitor Users gives you online, real-time information about Oracle E-Business Suite Forms and HTML-based session users. You can see:

- What users are signed on (by application user name and operating system login

name)

- Which responsibilities, forms (windows), and terminals they are using
- How long they have been logged in
- What Oracle database processes they are using
- The IP address of the client machine (starting with Release 12.2.10 and later or R12. ATG_PF.C.Delta.9)

Monitoring features include current and historic user activity down to the page access level and current and historical Concurrent Manager activity.

> **Important:** You can only monitor Forms for those users that are being audited by Sign-On Audit. The Application Monitor also reflects the level of auditing you define for your users.

In addition, you can monitor all users at a site, all users accessing a specific application or a specific responsibility, or individual users.

> **Note:** You can only monitor those users for whom you have activated Sign-On Audit.

Within the user interface, click **Audit Cleanup** to submit the concurrent program Disable Inactive Sessions (which is described in the following section).

There are two methods to access the Monitor Users application:

- To access the Monitor Users Forms-based application, navigate to navigate to **System Administrator** >**Security** >**User** >**Monitor**. Before using this form, select a value for the Sign-On:Audit Level profile option, using the Update System Profile Options window.
- Release 12.2.10 introduces the HTML-based Monitor Users application. To view this, navigate to **System Administration** >**User Monitor**.

Disabling Inactive Sessions

Use the Disable Inactive Sessions concurrent program to end sessions that may have been abandoned and exceed the ICX Limit Time. Run this concurrent program on a daily basis.

Disable Inactive Sessions can be submitted by clicking **Audit Cleanup** within the Monitor Users user interface. It can also be submitted by using the Submit Request form.

If user activity times out, the existing audit data associated with the session will be end dated. If the user re-authenticates and resumes the session, then the audit data will be updated on access. Any open forms and responsibilities will remain end dated until they are re-accessed.

Purging Session Information

Purge session information using the Purge Inactive Session (FNDDLTMP) concurrent program. This program purges all information for inactive sessions from the following tables:

- ICX_SESSIONS
- ICX_SESSION_ATTRIBUTES
- ICX_TRANSACTIONS
- ICX_TEXT
- ICX_CONTEXT_RESULTS_TEMP
- FND_SESSION_VALUES

R12.ATG_PF.C.Delta.9 introduces a new retention period for ICX_SESSIONS that specifies how much data from ICX_SESSIONS should be retained. This defaults to 400 days.

The Purge Inactive Session concurrent program also deletes unsuccessful login information older than 30 days from the ICX_FAILURES table.

The program also end dates any pending audit data associated with the session - see Disabling Inactive Sessions, page 16-7.

Purging Sign-On Audit Data

Purge end-user access data using the Purge Sign-On Audit Data (FNDSCPRG) concurrent program. This current program purges all Sign-On Audit information created before a specified date. Run this concurrent program between once a week and once a month.

R12.ATG_PF.C.Delta.10 introduces a new retention period that specifies how much data from the previously listed tables should be retained. This defaults to 400 days. Note that in R12.ATG_PF.C.Delta.10, the previous date concurrent parameter is no longer visible.

This concurrent program purges the following tables:

- FND_LOGIN_RESP_FORMS
- FND_LOGIN_RESPONSIBILITIES

- FND_LOGINS
- FND_UNSUCCESSFUL_LOGINS
- FND_APPL_SESSIONS

The following data is deleted:

- Data for who signs on and for how long
- Data for who is selecting what responsibility and when they do it
- Data for who uses which forms in an application and when

This program will delete all Sign-On Audit information created before specified by the audit date parameter.

Sign-On Audit Reports

Oracle E-Business Suite ships standard reports detailing which users are signing on; the responsibilities they are accessing; the forms they are using; concurrent requests they are submitting; and details of any attempts to log on to other users' accounts. The reports are accessible through the system administrator responsibility. Oracle E-Business Suite standard Sign-On Audit reports include the following:

- Sign-On Audit Concurrent Requests: shows concurrent requests and who submitted it
- Sign-On Audit Forms: shows all Forms and who accessed each Form
- Sign-On Audit Responsibilities: shows all responsibilities and who used it
- Sign-On Audit Unsuccessful Logins: shows the user id and the date of any unsuccessful logins
- Sign-On Audit Users: shows who signed on

For each report, you can also specify search criteria to customize the result set. Details regarding these reports are available in Appendix F: Sign-On Audit Concurrent Manager Reports, page F-1.

Session Audit Information

Although there are no prebuilt reports for reporting on OAF and JTF based applications, quite a lot of information is captured automatically in the login and session tables. These tables can be queried to retrieve information on what is currently happening in the system, or what was recently done.

- APPLSYS.FND_LOGINS
- APPLSYS.FND_LOGIN_RESPONSIBILITIES
- APPLSYS.FND_LOGIN_RESP_FORMS
- APPLSYS.FND_UNSUCCESSFUL_LOGINS
- ICX.ICX_FAILURES

See My Oracle Support Knowledge Document 2069190.1, *Security Configuration and Auditing Scripts for Oracle E-Business Suite*, for some example queries on these tables. These can be leveraged to determine what users are currently logged in, as well as what they are currently doing.

Page Access Tracking

Page Access Tracking in Oracle Applications Manager reports aggregate data for OAF- and JTF-based applications, with Sign-on Audit data gathered for Forms-based applications. Consequently, you can view usage flow paths that span all three technology stacks.

Page Access Tracking allows administrators to track application usage statistics and perform Web site traffic analysis, aggregate data about user flows as well as drill down to a particular user session.

Page Access Tracking transparently captures application-rich context information for every user click. In terms of performance, the data capture has negligible overhead.

In the Page Tracking Administration UI, You Can:

- Enable and disable Page Access Tracking
- Configure the granularity to which application context information is captured
- View reports on the gathered data

Examples of Available Reports:

- Access reports for a given application, responsibility and/or user across the Oracle Applications Framework, JTF, and Forms tech stacks
- Page Performance reports per application tier node
- Page access flow chart for a given user session
- Search reports based on several filter criteria

Configuring Page Access Tracking

Perform the following steps as described to configure Page Access Tracking for your site.

1. **Navigate to the UI.**

   Use the following navigation paths to reach the Page Access Tracking Configuration Page:

   Oracle Applications Manager: **Site Map** > **Monitoring** > **Applications Usage Reports** > **Page Access Tracking and Sign-on Audit Configuration**

2. **Turn Page Access Tracking on or off.**

   On the Page Access Tracking Configuration page, you can enable or disable Page Access Tracking for your site. This is the primary site-level switch for Page Access Tracking -- setting this field to Off overrides any other configurations.

3. **(Optional) Configure logging for responsibilities or users.**

   Optionally, you can configure logging according to user or responsibility. To do so, use Oracle Forms to set up the profile JTF_PF_ENABLED.

4. **Choose the applications to log.**

   On the Page Access Tracking Configuration page, use the shuttle to move applications between the Disabled and Enabled lists. Only enabled applications will be logged. (Alternatively, this step can be performed through Oracle Forms by setting up the JTF_PF_ENABLED profile.)

5. **Select request attributes.**

   On the Page Access Tracking Configuration page, you can choose how much data to collect by selecting one of the following combinations:

   - **Session Information** - Collected information from the Session Information setting which includes:
     - **Page Information** - Time stamp, JSP name (for example, `jtflogin.jsp`), JSP execution time, in milliseconds
     - **Server Host Information** - Host name, Apache port, Jserv port, Request method (such as POST, GET, PUT, HEAD), Return status (OK, Error, or Exception)
     - **Session Context** - Application ID, Responsibility ID, User ID, Language ID, Session ID
     - **Client Browser Information** - Client language, HTTP header, User-agent,

Protocol, Referer, Authorization type

- **Client Language Information** - Character coding, Language, Character set

- **Session Information and Cookies** - Includes session information plus all incoming cookies.
- **Session Information, Cookies, and URL Parameters** - Includes session information, all incoming cookies, and any GET parameters.
- **Session Information, Cookies, and All Parameters** - Includes session information, all incoming cookies, any GET parameters, and any POST parameters.

Oracle recommends that the Request Attributes be set to Session Information for normal auditing purposes. The other settings can end up logging sensitive data, and are only appropriate for diagnostic purposes.

6. **Apply your changes.**

   To apply the configuration changes that you have made, restart all the JVMs that use or will use Page Access Tracking.

Migrating Page Access Tracking Data

Page Access Tracking data is logged in the database in a staging area. It needs to be migrated and mined before the UI reports are refreshed. How frequently Page Access Tracking Data needs to be migrated and mined depends on how up-to-date the UI reports need to be. Generally speaking, the recommendation is to run the concurrent program at least once a day (for example at midnight) for the reports to be relatively up to date.

Page Access Tracking Data Migration can be scheduled either in Oracle Forms, or within the OAM responsibility.

Schedule the concurrent program Page Access Tracking Data Migration using Concurrent Manager:

After the concurrent program completes, you should be able to view the latest data reports and statistics.

Viewing Page Access Tracking Reports

1. **Locate the UI.**

   To reach the Page Access Tracking Reports page in Oracle Applications Manager, go to: **Site Map**, the select **Monitoring**, then **Applications Usage Reports**, and then **Page Access Tracking and Sign-on Audit Reports**.

2. **View reports and report details.**

   The default report provides statistical summaries for the past week of application usage as well as application tier usage.

   Application Usage includes: Number of page hits, Sessions, Unique users, Unique applications, Unique responsibilities, and Languages.

   For each of these statistics, you can drill down to view the respective Details page.

   To see a table or graph of a complete session page flow, click an individual session ID on the Session Details page. The page indicates which tech stack each access belongs to. If during a session a user accesses both JSPs and Forms across tech stacks (Oracle Applications Framework and/or Oracle Forms), the Session Details page shows the complete flow across the tech stacks, from login to logout.

   > **Note:** In the summary page, a tech stack of FORMS displays when the source is sign-on auditing. However, this data may be generated via Oracle Application Framework and Oracle CRM Technology Foundation technology stacks, and so get incorrectly reported as FORMS. The drill down correctly reports these as AUDIT.
   >
   > In session drill down, the login is sometimes repeated multiple times in the table. The graph view resolves this issue.

   Querying the Page Access Tracking tables directly may, depending on what your requirements are, be more convenient and provide a mechanism for preserving historical auditing data. This can be used to query and provide a record of users that access sensitive pages (for example, the sensitive administration pages referenced in My Oracle Support Knowledge Document 1334930.1, *Sensitive Objects and Administrative Pages in Oracle E-Business Suite*), or to track the UI page flow activities of applications administrators (for example, SYSADMIN).

   See My Oracle Support Knowledge Document 2069190.1, *Security Configuration and Auditing Scriptsfor Oracle E-Business Suite*, for some example scripts that query the Page Access Tracking tables directly.

   Application Tier Usage includes: Host name, Server port, Number of JVMs, Average page execution time, Page hits, and Page failures.

   To define a specific date range, click **Edit**.

3. **Set the flush interval and maximum buffer size.**

   Page Access Tracking data is buffered within each JVM and periodically asynchronously flushed to the database. The flush is triggered by the following site-level profiles:

   - JTF_PF_FLUSH_INTERVAL, which defines a time interval. The default value is 120 seconds.

- JTF_PF_BUFFER_SIZE, which defines the maximum number of page log accesses in the buffer. The default value is 20 accesses.

The data is flushed to the database when the specified time interval is reached, or when the number of page log accesses exceeds the configured buffer size. These parameters can be modified from their default values through Oracle Forms. The default values are used if the profiles are not set.

4. **Purge Page Access Tracking repository.**

   The amount of data recorded by Page Access Tracking depends on what applications, responsibilities and users have tracking turned on, the tracking level selected and user traffic. On a regular basis, the System Administrator should purge the Page Access Tracking repository. The frequency of data purge also depends on how much historical tracking data is needed in the UI reports.

   Schedule the concurrent program Page Access Tracking Purge Data using Concurrent Manager.

Database Connection Tagging

The Database Connection Tagging feature utilizes several Oracle Database session attributes that allow Oracle E-Business Suite to record the database connection's current use. The Database Connection Tagging feature is controlled by the profile option FND: Connection Tagging (FND_CONNECTION_TAGGING).

By default, the profile option value is set to 'Enabled' (recommended), so Oracle E-Business Suite database connections are tagged with the information described in the previous section. If the feature is disabled, database connections will not be tagged and no information will be collected.

The CLIENT_IDENTIFIER, MODULE, and ACTION columns of the V$SESSION database table are used to track user and application context. These columns are populated as follows:

- **CLIENT_IDENTIFIER** - The client for a particular database session. The value allows the end user of that database connection to be identified. For context-insensitive standalone modules such as FNDLOAD or FNDCPASS, the value of CLIENT_IDENTIFIER is set to 'SYSADMIN'.

- **MODULE** - Name of the currently executing module. The value indicates the application code where the database workload originates, and consequently allows identification of the specific application code (such as a user interface, program, or web service) that is currently using the connection.

- **ACTION** - Name and context of the currently executing business action; for example, a payroll task being undertaken by a particular responsibility.

Note: This information is captured, and can be leveraged in Database Auditing, and will automatically be populated in Oracle Database Vault and Database Firewall if using that product.

You can also leverage this information for querying the v$session table for a specific FND user or for specific pages. For example you can query the v$session for SQL being currently by a current FND User, or for a particular page. See My Oracle Support Knowledge Document 2069190.1, *Security Configuration and Auditing Scripts for Oracle E-Business Suite*, for additional scripts that leverage the Database Connection Tagging in v$session.

Example:

```
Query select to_char(logon_time,'DD-MON-RRRR HH:MI:SS'),sid,
client_identifier, module,action

from v$session

where client_identifier = '&fnd_user';


Results

LOGON_DATE             SID FND_USER   MODULE
ACTION

16-OCT-2015 05:49:39    50 JFROST     e:PER:fwk:per.selfservice.common.
server.CommonAM   PER/EMPLOYEE_DIRECT_ACCESS_V4.0


16-OCT-2015 05:48:41   180 JFROST     e::fwk:fnd.framework.service.
lookups.server.Look   /
```

Debug Logging (Unexpected Logging)

Note: This section covers the profile settings required to write recommended auditing and logging information to log files. For settings and requirements to write logging messages to the screen, see "Enabling Logging to Screen in Oracle Application Framework Pages" in the *Oracle E-Business Suite Maintenance Guide*.

The Oracle E-Business Suite debug log set by the profile option "FND: Debug Log Enabled" is used for a variety of purposes. As the name suggests, it is often used for diagnosing and debugging problems encountered in Oracle E-Business Suite code. This log can assist with diagnosing security problems, detecting security attacks, and can also be leveraged for post-attack, or forensic analysis, or both.

The debug log is documented in "Using Oracle Application Object Library Profile Options to Configure Logging" in the *Oracle E-Business Suite Maintenance Guide*. The current recommendation is to set FND: Debug Log Enabled to UNEXPECTED. This is

important from a security auditing perspective, since this is the level at which many of the security errors are written out to the log.

The default configuration (and the current recommendation) for Debug Logging is set to log information to the database. This makes it easier to correlate and maintain logs in a multi-tier application environment.

The Debug Logging mechanism also supports logging to the file system using the following profile:

Debug Logging Profile Option

Profile Option Name	Code (Internal Name)	Value
FND: Debug Log Filename	AFLOG_FILENAME	`/path/to/apps.log`

Customers may want to consider enabling logging on the file system, as there are some security benefits to maintaining the log on the file system. File system logging will generally provide better protection against an attacker being able to modify logging records by using a SQL injection attack.

Oracle E-Business Suite Audit Trail

Oracle E-Business Suite has its own auditing mechanism called Audit Trail. Audit Trail lets you keep a history of changes to your important data: what changed, who changed it, and when. This feature keeps a complete history of changes made at a table and column level. With Audit Trail, you can easily determine how any data row or element obtained its current value. You can track information on most types of fields, including character, number and date fields.

When you enter or update data in Oracle E-Business Suite, you change the database tables underlying those forms. Audit Trail tracks which rows in the database were updated at what time, and which user was logged in using the associated form(s).

Audit Trail stores change information in a shadow table of the audited table. This mechanism saves audit data in an uncompressed but sparse format, and you enable auditing for particular tables and groups of tables (audit groups).

Additional details for enabling the Audit Trail are found in Enabling Oracle E-Business Suite Audit Trail, page 18-1.

17

Oracle E-Business Suite Technology Stack Auditing and Logging Features

Introduction

This chapter covers specifics for auditing and logging the various components of the Oracle E-Business Suite application and database tier technology stack.

Application Tier Technology Stack

Fusion Middleware Oracle HTTP Server (OHS)

The HTTP server delivered with Oracle E-Business Suite is an Apache based server called Oracle HTTP Server (OHS). The logging directives available for OHS are similar to the standard directives delivered with Apache.

Oracle E-Business Suite Release 12.2 uses an Apache 2.2 based OHS from the Fusion Middleware (FMW) 11R1g bundle. FMW can be configured to use one of two specific logging modes. Oracle E-Business Suite uses the ora-text mode.

OHS by default writes three log files: the console log, the access log and the error log.

The logging directives for OHS are defined in the `httpd.conf` and `security2.conf` files.

All OHS log files are written to the [component]/instance directory.

OHS Console Log

OHS writes general logging information to a main log file called `console~OHS~1.log` . The content of the log file is not configurable. The information written here includes:

- Start and stop of the OHS instance

- Any warnings about the OHS configuration observed during startup

  Note: In a standard Apache environment, this information would be written to the error log file.

  Note: If the following messages from ModSecurity Version 2.7 are observed in the log file, they can be ignored:

```
ModSecurity: WARNING Using transformations in
SecDefaultAction is deprecated \


(/u01/install/APPS/fs1/FMW_Home/webtier/instances/EBS_web_
EBSDB_OHS1/config/OHS/EBS_web_EBSDB/security2.conf:49).

 ModSecurity: WARNING Using transformations in
SecDefaultAction is deprecated \


(/u01/install/APPS/fs1/FMW_Home/webtier/instances/EBS_web_
EBSDB_OHS1/config/OHS/EBS_web_EBSDB/security2.conf:71).
```

OHS Access Log

All requests processed by OHS are logged in the access_log file. The location and content of access_log are defined by the LogFormat and CustomLog directives in the `httpd.conf` file. Oracle E-Business Suite uses the standard common format as follows:

```
LogFormat "%h %l %u %t \"%r\" %>s %b" common

 CustomLog "|${ORACLE_HOME}/ohs/bin/odl_rotatelogs ${ORACLE_INSTANCE}
/diagnostics/logs/${COMPONENT_TYPE}/${COMPONENT_NAME}/access_log 43200"
common
```

The fields in the log file correspond to the following:

```
%h - the IP address of the requesting client
%l - "ident" of requesting user (never used, always '-')
%u - logged in user (always '-' unless Basic-Auth is used)
%t - timestamp in square brackets - including time zone
%r - the requested URL path - including any querystring
%>s - the HTTP status code
%b - number of bytes in the response body
```

The following is an example log line:

```
172.17.122.44 - - [10/Aug/2015:17:53:52 -0400] "GET /page.jsp?p1=search
HTTP/1.0" 200 1197
```

OHS Error Log

The error_log is handled by the Oracle specific odl-text mode by default. This logging mode is controlled by the following directives:

```
OraLogDir "${ORACLE_INSTANCE}/diagnostics/logs/${COMPONENT_TYPE}
/${COMPONENT_NAME}"
OraLogMode odl-text
OraLogSeverity WARNING:32
OraLogRotationParams S 10:70
```

The default name for the error_log file is "$COMPONENT_NAME," such as `EBS_web_<SID>.log`, where SID is the database SID for the environment.

The format of error log is normally quite free form. OHS's error log however logs many fixed fields as seen in the following example:

```
[2015-08-03T14:37:29.4226-04:00] [OHS] [ERROR:32] [OHS-9999] [core.c]
[host_id: apps.example.com] [host_addr: 172.17.122.44]
 [tid: 139782812313344] [user: oracle] ecid:
005AcAsWJ122RPKLQUt1id0000Wx0002GF] [rid: 0] [VirtualHost: main] File
does not exist:
/u01/install/APPS/fs1/inst/apps/EBSDB_apps/portal/favicon.ico, referer:
http://apps.example.com:8000/
```

OHS HTTPS Log

When OHS is HTTPS enabled, requests received on the HTTPS port will also be logged to ssl-specific log files. These log files and their format is defined in `ssl.conf`.

> **Note:** If you have not already done so, you should enable TLS. Refer to My Oracle Support Knowledge Document 1367293.1, *Enabling TLS in Oracle E-Business Suite Release 12.2.*

The HTTPS-specific log entries are written to the `ssl_request_log` file and defined by the following directives in the `ssl.conf` file:

```
CustomLog "|${ORACLE_HOME}/ohs/bin/rotatelogs \
  ${ORACLE_INSTANCE}/diagnostics/logs/${COMPONENT_TYPE}
/${COMPONENT_NAME}/ssl_request_log 86400" \
  "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
```

The `ssl_request_log` file will record the SSL protocol and CipherSuite used for the connection.

The fields in the log file correspond to the following:

- `%t` - timestamp in square brackets - including time zone
- `%h` - the IP address of the requesting client
- `%{SSL_PROTOCOL}x` - The protocol
- `%{SSL_CIPHER}x` - the CipherSuite
- `%r` - the requested URL path - including any querystring
- `%b` - number of bytes in response body

The following is an example line from the log file:

```
[10/Aug/2015:17:53:52 -0400] 172.17.122.44 TLSv1.2
SSL_RSA_WITH_AES_256_GCM_SHA384 "GET / HTTP/1.0" 1197
```

Other OHS Logging

OHS also loads additional modules that may generate log output if explicitly enabled. They are mod_security and mod_rewrite.

Mod_security will write log information to the Apache error log file. In Oracle E-Business Suite Release 12.2, the log file is named `EBS_web_<SID>.log`, where <SID> is the SID of the database. By default, mod_security will add log entries to this log file whenever it denies a request.

The following is an example of mod_security logging to the error log:

```
[2015-08-03T14:37:29.4226-04:00] [OHS] [ERROR:32] [OHS-9999] [core.c]
[host_id: apps.example.com] [host_addr: 172.17.122.44]

 [tid: 139782812313344] [user: oracle] [ecid:
00576lqFfjS1rYHqysfd6G0000V700028o] [rid: 0] [VirtualHost: main]
[client 10.211.207.102]

 ModSecurity: Access denied with code 400 (phase 2). Pattern match
"['<>\\";\\\\\\\\]" at ARGS:locale.

 [file
"/u01/install/APPS/fs1/FMW_Home/webtier/instances/EBS_web_EBSDB_OHS1/con
fig/OHS/EBS_web_EBSDB/security2.conf"] [line "63"] [id "100020"]

 [hostname "apps.example.com"] [uri "/OA_HTML/help/state"] [unique_id
"Vb@06awReiwAAAioEm0AAAAF"]
```

ModSecurity can also generate audit and debug logging information in separate log files defined in `security2.conf`.

ModSecurity audit logging are off by default. Audit logging can be turned by setting the following parameter in `security2.conf`, then bouncing the Apache server:

```
SecAuditEngine On
```

ModSecurity audit logging is written to the sec_audit_log file. Information in the audit_log is useful for diagnostic purposes as it will log the full request and the response headers. All parameters, including the POST payload of the request, are available.

> **Caution:** Be careful if enabling this audit logging feature. Many of the logged parameters may be considered sensitive. ModSecurity in Oracle E-Business Suite Release 12.2 blanks out a number of well-known password parameters before writing the log entry; however, there is other information that may be considered sensitive. You should consider the audit log as highly sensitive and restrict access.

ModSecurity debug logging is off by default and should not be enabled. If enabled, it can be used for debugging rules in `security2.conf`. Debug logging if enabled is written to the sec_debug_log file.

Similarly mod_rewrite has a debug log file called `mod_rewrite.log`. Mod_rewrite debug logging is disabled by default and should not be enabled. If enabled, it can used for debugging mod_rewrite actions from any of the OHS .conf files.

Oracle Database

Database Listener

The listener log file contains audit trail information that enables you to collect and analyze network usage statistics, as well as information indicating the following:

- A client connection request
- A `RELOAD`, `START`, `STOP`, `STATUS`, or `SERVICES` command issued by the Listener Control utility

You can use the audit trail information to view trends and user activity by first storing it in a table and then collating it in a report format. To import the data into a table, use an import utility such as SQL*Loader.

Format of the Listener Log Audit Trail

Audit Trail formats text into the following fields:

```
Timestamp * Connect Data [* Protocol Info] * Event [* SID | Service] *
Return Code
```

For more information, refer to "Analyzing Listener Log Files" in the *Oracle Database Net Services Administrator's Guide*.

Enable TNS Listener Logging

To enable logging, in `$TNS_ADMIN/listener.ora`, set the following parameters:

```
LOG_STATUS = ON
LOG_DIRECTORY_$ORACLE_SID = $TNS_ADMIN
LOG_FILE_$ORACLE_SID = $ORACLE_SID

 For example,
LOG_STATUS = ON
LOG_DIRECTORY_VIS12 = /u/db/tech_st/10.2.0/network/admin/VIS12_dbs01
LOG_FILE_VIS12 = VIS12
```

Where VIS12 is the LISTENER_NAME.

> **Note:** This configuration is done by default with Oracle E-Business Suite Release 12.2.

Database Alert Log

The alert log is an XML file that is a chronological log of messages and errors. For the database, the alert log includes messages about the following:

- Critical errors (incidents)
- Administrative operations, such as starting up or shutting down the database, recovering the database, creating or dropping a tablespace, and others.
- Errors during automatic refresh of a materialized view
- Other database events

For more information, see "Managing Diagnostics Data" in the *Oracle Database Administrator's Guide*.

The alert log is a chronological log of messages and errors, and includes the following items:

- All internal errors (ORA-00600), block corruption errors (ORA-01578), and deadlock errors (ORA-00060) that occur
- Administrative operations, such as CREATE, ALTER, and DROP statements and STARTUP, SHUTDOWN, and ARCHIVELOG statements
- Messages and errors relating to the functions of shared server and dispatcher processes
- Errors occurring during the automatic refresh of a materialized view
- The values of all initialization parameters that had nondefault values at the time the database and instance start

For more information, refer to "Monitoring the Database" in the *Oracle Database Administrator's Guide*.

Database Auditing

Database auditing includes monitoring and recording of configured database actions. You can base auditing on individual actions, such as the type of SQL statement processed, or on combinations of data that can include the user name, application, time, and so on.

Unified Auditing is recommended for Oracle E-Business Suite Release 12.2.11 or for Oracle E-Business Suite Releases 12.2.3 through 12.2.10 with the application of the EBS System Schema Migration Consolidated Patch. See My Oracle Support Knowledge Document 2777404.1, *Enabling Unified Auditing in Oracle E-Business Suite Release 12.2*

with Oracle Database 19c or 12c, for more information.

Traditional auditing is recommended for Oracle E-Business Suite releases prior to 12.2.11 if the minimum required for Unified Auditing with Oracle E-Business Suite Release 12.2 have not been met. See My Oracle Support Knowledge Document 2793599.1, *Traditional Database Auditing with Oracle E-Business Suite Release 12.2*, for more information.

Any additional database auditing configured beyond what is recommended in the aforementioned My Oracle Support knowledge documents generate significant entries of little value. Oracle E-Business Suite dynamically creates, alters, and drops objects (tables, index, packages, and so forth) on a regular basis. Auditing additional actions provides little meaningful information and could affect the performance of your environment.

Optional Oracle Technology Integrations

Oracle Audit Vault and Database Firewall

Oracle Audit Vault automates the consolidation of audit data into a secure repository, enabling efficient monitoring and reporting. Oracle Audit Vault is a powerful solution providing a secure repository, built-in reporting, event alerting, and separation-of-duty. Built on Oracle's industry leading technology, Oracle Audit Vault uses Oracle data security to protect audit data end-to-end. The latest release of Oracle Audit Vault provides enhanced out-of-the-box compliance reporting and audit collection, including support for Microsoft SQL Server 2000 & 2005, IBM DB2 Unix, Linux, and Windows 8.2 & 9.5, and Sybase ASE 12.5 & 15.0 databases.

Central to Oracle Audit Vault is a secure data repository built on Oracle's industry leading data warehousing technology and secured with Oracle's industry leading security products. Built-in reporting and event alerting help businesses improve their ability to comply with external regulations and internal policies by lessening the time and effort required to detect potential problems and demonstrate that mandated controls are in effect and working. Data security administrators and auditors can manage, compare and provision Oracle database auditing settings across the enterprise directly from the Oracle Audit Vault console, lowering overall maintenance costs.

Security and Scalability

Audit data is an important record of business activity. Audit data must be protected against modification to ensure the integrity of reports and investigations based on the audit data. Oracle Audit Vault stores audit data in a secure repository built using Oracle's industry leading database security technology. Timely transfer of audit data from source systems to Oracle Audit Vault is critical to close the window on intruders who may attempt to modify audit data and cover their tracks. Oracle Audit Vault can be configured to transfer audit data on a near real time basis. Oracle Audit Vault protects audit data during transfer over the network and within Oracle Audit Vault.

During transfer from the source systems, audit data can be encrypted, preventing anyone from reading or tampering with the data during transmission.

Inside Oracle Audit Vault access to audit data is strictly controlled based on the principle of separation-of-duty. Oracle Real Application Clusters (RAC) can optionally be licensed for Oracle Audit Vault, enabling additional scalability and high availability.

- Consolidate database audit trail into secure centralized repository
- Detect and alert on suspicious activities, including privileged users
- Out-of-the box compliance reports for SOX, PCI, and other regulations
  - For example: privileged user audit, entitlements, failed logins, regulated data changes
- Integrate with Oracle E-Business Suite security system
- Monitor inbound SQL activity in passive mode
- Alert security operations of unexpected activity
- Run standard or develop custom reports

Fine-Grained Auditing

Fine-grained auditing allows detailed conditions to trigger auditing. Policies you establish with fine-grained auditing can monitor data access based on content. Using policies, you can specify the columns and conditions that you want audit records for (for ex: all access to a salary table with the salary is greater than X amount). Conditions can include limiting the audit to specific types of DML statements used in connection with the columns that you specify.

In general, fine-grained audit policies are based on simple, user-defined SQL predicates on table objects as conditions for selective auditing. During fetching, whenever policy conditions are met for a row, the query is audited.

You can use fine-grained auditing to audit the following types of actions:

- Accessing a table between 9pm and 6am or on Saturday and Sunday
- Using an IP address from outside the corporate network
- Selecting or updating a table column
- Modifying a value in a table column

Fine-grained auditing creates a more meaningful audit trail, one that includes only very specific actions that you want to audit. It excludes unnecessary information that occurs if each table access was recorded. For more information, refer to "About Fine-Grained

Auditing" in the *Oracle Database Security Guide*.

18

Enabling Oracle E-Business Suite Audit Trail

Overview

> **Note:** The content in this chapter is maintained for historical purposes. We recommend you use Oracle Database Unified Auditing. For more information, see Database Auditing, page 17-6.

You can choose to store and retrieve a history of all changes users make on a given table. Auditing is accomplished using audit groups, which functionally registered Oracle IDs or group tables to be audited. For a table to be audited, it must be included in an enabled audit group.

Audit Trail Groups are groups of tables and columns. You do not necessarily need to include all the columns in a given table. You enable auditing for audit groups rather than for individual tables. You would typically group together those tables that belong to the same business process (for example, purchase order tables).

A given table can belong to more than one audit group. If so, the table is audited according to the highest level of enabling for any of its groups, where Enabled is the highest, followed by Disable Dump Data, Disable No Growth, and Disable Purge Table, in that order.

You can enable auditing for a maximum of 240 columns for a given table, and you can enable auditing for all types of table columns except LONG, RAW, or LONG RAW. Your audit group must include all columns that make up the primary key for a table; these columns are added to your audit group automatically. Once you have added a column to an audit group, you cannot remove it.

> **Note:** Do not include too many columns for a table. Audit Trail constructs a view creation SQL statement using the columns, and this

statement is subject to a size limitation. The limitation on the maximum length for a SQL statement depends on many factors, including database configuration, disk space, and memory. For more information, see the Oracle Database documentation.

Steps to Enable Audit Trail

To enable Oracle E-Business Suite Audit Trail, review and perform the following steps as required:

1. **Granted required privileges.**

   Have your database administrator grant SELECT privileges on SYS.DBA_TABLES to the APPLSYS account. Normally, this step will already have been done as part of the installation or upgrade.

2. **Register custom tables and primary keys.**

   Your tables and their primary key information must already be registered and defined for successful auditing. If the table you want to audit is a custom table (not shipped as part of Oracle E-Business Suite), you should also perform the following two steps:

   1. Register your table and its primary key columns using Oracle Application Object Library's Tables window (Application Developer Responsibility).

   2. Run the Register Tables concurrent program from the Submit Requests window.

3. **Turn on Audit Trail.**

   Turn on Oracle E-Business Suite Applications Audit Trail by setting the system profile Audit Trail: Activate to True

4. **Define Audit Installations (optional).**

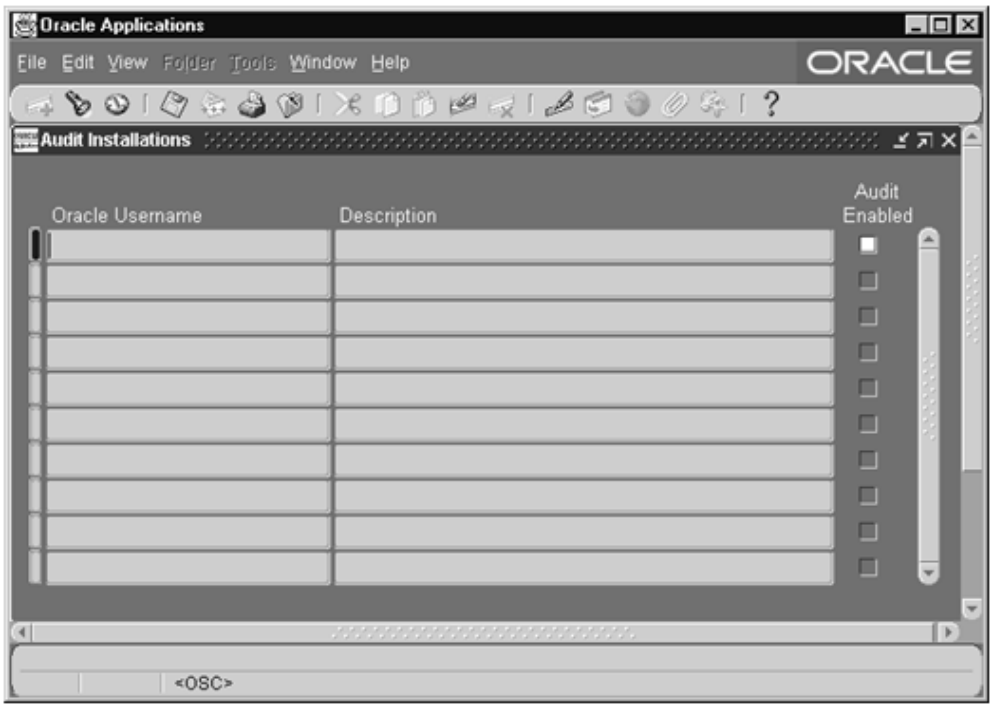
   You may optionally choose to audit by a registered Oracle ID. This allows you to audit across multiple application installations. When a table is added to an audit group, auditing will automatically be enabled for all installations of the table for which audit is enabled.

   Before you proceed, ensure that the desired Oracle user name is registered. The installation process automatically registers Oracle E-Business Suite Oracle user names, but if you create a custom application, you should follow instructions in My Oracle Support Knowledge Document 1577707.1, *Creating a Custom Application in Oracle E-Business Suite Release 12.2*, for Oracle user names for custom applications.

   To audit by a registered Oracle ID, do the following:

Navigate through **Security** > **Audit Trail** > **Install** and select the registered Oracle user names at your site that you wish to audit. Select the **Audit Enabled** checkbox to enable Audit Trail for an Oracle user name.

Audit Installations Window



For auditing to take effect, you must perform the next steps in this section.

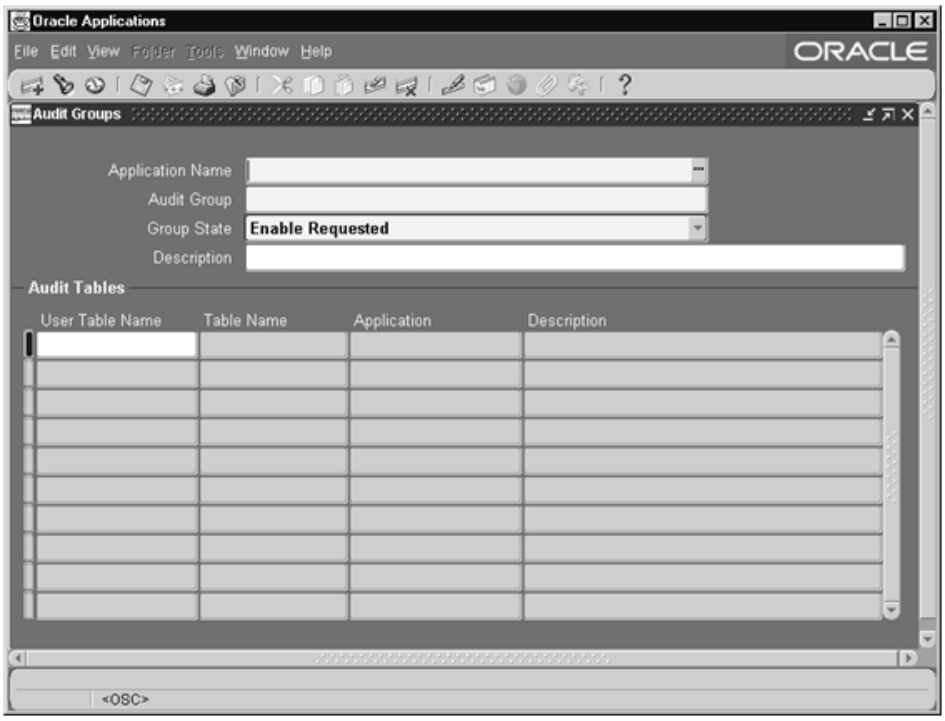
5. **Define Audit Groups.**

   You can audit a table or Oracle ID by defining an audit group, which can consist of one or more tables. To create an Audit Group and assign specific tables and columns, perform the following:

   1. Navigate to **Security** > **Audit Trail** > **Groups** to create audit groups and set tables to be audited. Set audit group to Enabled Requested.

   2. Identify the tables you want to audit or tables owned by an Oracle ID selected for auditing in the previous step, Define Audit Installations. See Tables to Audit with Audit Trail, page 18-10 for a list of recommended tables to consider auditing.

Audit Groups Window



- Audit Groups block - Identify your audit group and enable or disable auditing for this group.
- Application Name - Select the name of an application to associate with your audit group. The combination of application name and group name uniquely identifies your audit group. An audit group may be used to audit tables in additional applications.
- Audit Group - Enter the name of the audit group.
- Group State - Choose Enable Requested if you are defining a new audit group. When you run the Audit Trail Update Tables report, the concurrent program creates database triggers for the tables in your audit group. Once you have run the program, this field displays Enabled for audit groups where Audit Trail is active.

  Important: All primary key columns in each table in an audit group are automatically selected for auditing, whether or not you use the Audit Tables window to select which columns you wish to audit.

6. **Activate Audit Trail.**

Your Audit Trail definitions (and auditing) do not go into effect until you run the Audit Trail Update Tables Report. If you change any of your definitions later, you must rerun this program. Submit the Audit Trail Update Tables concurrent request from the standard submission (Submit Reports) form.

Audit Trail Shadow Tables, Triggers, and View

Upon execution, the Audit Trail Update Table concurrent request performs the following tasks:

- Creates shadow tables, one for each audited table, to contain the audit information.
- Creates database triggers on the tables in your audit groups for your installations.
- Creates two views for each column with the names _AC# and _AV# where # is a sequential number.

Each of these tasks is described in detail in the following sections.

Shadow Tables

The shadow table is automatically created in the same Oracle ID as the audited table. The shadow table name contains the first 24 characters of the audited table name plus "_A" (Audit). For example, the Audit Trail shadow table is named as follows: Audit Trail shadow table name = <table_name>_A

The shadow table contains only the columns to be audited, and all columns in the shadow table are unconstrained, regardless of their status in the table to be audited. For example, NULLs are always permitted in the shadow table. All columns in the shadow table have the same data types and sizes as their counterparts in the audited table.

All Audit Trail shadow tables contain certain special auditing columns. These columns include:

- AUDIT_USER_NAME (the Application User ID, except when changes are applied using SQL*Plus, in which case it is the Oracle ID).
- AUDIT_TIMESTAMP (the date/time when the insertion occurred).
- AUDIT_TRANSACTION_TYPE (I for Insert, U for Update, D for Delete, L for Last, and C for Current).
- AUDIT_TRUE_NULLS (VARCHAR2(250) column containing a delimited list of column names that have changed from NULL).
- The primary key for the table. This is not a special column, but rather all the columns comprising the primary key of the audited table. Note that, by convention, all audited columns are stored when a row is deleted. Likewise, an insert results in

a row of NULL values in the shadow table. Changes to the primary key are marked as deletes, but new primary key values are inserted also.

For example, suppose you have the following table:

```
SQL> DESCRIBE AUDIT_DEMO

 NAME            NULL?    TYPE
 --------------- -------- ----
 PRIMARY_KEY              NUMBER(5)
 VALUE_ONE                VARCHAR2(5)
 VALUE_TWO                VARCHAR2(5)
 VALUE_THRE               VARCHAR2(5)
```

Its shadow table is as the following (assuming you audit all your table columns):

```
SQL> DESCRIBE AUDIT_DEMO_A

NAME                      NULL?       TYPE
----------------------    --------    ----
AUDIT_TIMESTAMP           NOT NULL    DATE
AUDIT_TRANSACTION_TYPE    NOT NULL    VARCHAR2(1)
AUDIT_USER_NAME           NOT NULL    VARCHAR2(100)
AUDIT_TRUE_NULLS                      VARCHAR2(250)
AUDIT_SESSION_ID          NOT NULL    NUMBER
AUDIT_SEQUENCE_ID         NOT NULL    NUMBER
AUDIT_COMMIT_ID           NOT NULL    NUMBER
PRIMARY_KEY                           NUMBER
VALUE_ONE                             VARCHAR2(5)
VALUE_TWO                             VARCHAR2(5)
VALUE_THREE                           VARCHAR2(5)
```

Database Triggers

When auditing is enabled, the automatically-generated database trigger in the "After" event on the audited table performs the auditing. The trigger calls a stored procedure to compare each column being audited to see if its value is changing. If so, the procedure saves the previous (old) value to the shadow table.

Auditing creates one row in the shadow table for each audited transaction against the table; thus, a single row in the shadow table represents all old values for all changed columns on that transaction.

The data is not compressed, since a table uses only one byte for a NULL, and Audit Trail represents all unchanged values as NULLs in the shadow table ("sparse" format).

The audit trigger names contain the first 24 characters of the audited table name plus "_AI," "_AU," or "_AD," where one of I, U or D indicates Insert, Update or Delete, respectively. Likewise, the audit procedure names use the first 24 characters of the table name plus "_AIP," "_AUP," or "_ADP." Your table names must be unique within the first 24 characters.

For example, the Audit Trail triggers are named as follows:

```
Audit Trail Update Trigger name = <table_name>_AU
Audit Trail Insert Trigger= <table_name>_AI
Audit Trail Insert Trigger= <table_name>_AD
```

Two Views for Each Column

After a shadow table is created, views onto the shadow table are created to allow easier access to the data in the "sparse" rows. These views simplify tasks such as querying a row/column's value on a given date and tracking changes to a row/column over time.

The view name contains the first 24 characters of the audited table name plus "_AC#" or "_AV#" where C or V indicates the type of view and # indicates a number. Due to limitations in creation size, the shadow table columns may need to be broken into multiple views, which are numbered sequentially.

For example, the Audit Trail views are named as follows:

Changes View = <table name>_AV#

Complete View = <table name>_AC#

Each view allows slightly different access to the data. One allows the user to reconstruct the value for a row at a given time (_AC), while the other provides simple access to when a value was changed (_AV).

For our example table, the _AV1 and _AC1 views are created as follows:

```
SQL> DESCRIBE AUDIT_DEMO_AV1

NAME                          NULL? TYPE
----------------------------  ----- ----
PRIMARY_KEY                         NUMBER
AUDIT_TIMESTAMP                     DATE
AUDIT_SEQUENCE_ID                   NUMBER
AUDIT_SESSION_ID                    NUMBER
AUDIT_TRANSACTION_TYPE              VARCHAR2(1)
AUDIT_USER_NAME                     VARCHAR2(100)
VALUE_ONE                           VARCHAR2(5)
VALUE_TWO                           VARCHAR2(5)
VALUE_THREE                         VARCHAR2(5)

SQL> DESCRIBE AUDIT_DEMO_AC1

NAME                          NULL? TYPE
----------------------------  ----- ----
PRIMARY_KEY                         NUMBER
AUDIT_TIMESTAMP                     DATE
AUDIT_SEQUENCE_ID                   NUMBER
AUDIT_SESSION_ID                    NUMBER
AUDIT_TRANSACTION_TYPE              VARCHAR2(1)
AUDIT_USER_NAME                     VARCHAR2(100)
AUDIT_COMMIT_ID                     NUMBER
VALUE_ONE                           VARCHAR2(5)
VALUE_TWO                           VARCHAR2(5)
VALUE_THREE                         VARCHAR2(5)
```

Purging Audit Trail Records

Purge the audit trail information on a regular basis. Prior to purging, disable the Audit Trail. Use the following procedure to purge audit data:

1. As System Administrator, select **Security** > **Audit Trail** > **Groups**.
2. Select the Security Audit group and set the group state to Disable - Purge Table.
3. Run the Audit Trail Update Tables Report.
4. Purge the data from the shadow table.
5. Select **Security** > **Audit Trail** > **Groups**.
6. Select the Security Audit group and set the group state to Enable.
7. Run the Audit Trail Update Tables Report.

Disabling an Enabled Audit Trail

You may disable auditing at any time. When you disable auditing, you should do the following procedure:

1. **Stop auditing new transactions.**

   Disable auditing using either "Disable - Prepare for Archive" or "Disable - Interrupt Audit" and running the Audit Trail Update Tables report.

Variable Descriptions

Variable	Description
Disable - Prepare for Archive	Copies the current values of all rows in the audited table into the shadow table, and then disables the auditing triggers. This option requires the most space, since there is at least one row in the shadow table for every row in the audited table (and another row in the shadow table for each transaction on the original row in the audited table). You should then archive the table before you empty the shadow table.

Variable	Description
Disable - Interrupt Audit	Modifies the triggers to store one final row in the shadow table as the audited row is modified in the audit table (remember that a given row in the shadow table represents the data in the audited row before an update). Inserts or further changes are no longer audited. The shadow table then grows slowly, and the data may be accessed by the existing audit views.
Disable - Purge Table	Drops the auditing triggers and views and deletes all data from the shadow table.

2. **Archive your audit data.**

   You should archive the information in the shadow tables according to your business needs.

3. **Clean out the shadow table.**

   Before you restart auditing, you should clean out the shadow table. If there were transactions during the time auditing was disabled, and you did not clean out the shadow table, the data in the shadow table would be invalid because it would have a gap where transactions were not recorded. You purge the shadow table(s) by setting the audit group to Disable - Purge Table and running the Audit Trail Update Tables report.

   Variable Descriptions

Variable	Description
Disable - Purge Table	Drops the auditing triggers and views and deletes all data from the shadow table.

Restarting an Audit

If desired, you can restart auditing by setting the audit group to Enable Requested and running the Audit Trail Update Tables report again.

Important: If you disable using Disable Purge Table and then re-enable

auditing for a table, Audit Trail flushes the contents of the shadow table when auditing is re-enabled. You should archive any shadow table data that you want to keep before you re-enable auditing.

Tables

Tables to Audit with Audit Trail

When enabling Audit Trail, you should consider auditing tables that control Oracle E-Business Suite system security. The following is a list of tables you should consider auditing:

- ALR_ALERTS
- FND_AUDIT_COLUMNS
- FND_AUDIT_GROUPS
- FND_AUDIT_SCHEMAS
- FND_AUDIT_TABLES
- FND_CONCURRENT_PROGRAMS
- FND_DATA_GROUPS
- FND_DATA_GROUP_UNITS
- FND_ENABLED_PLSQL
- FND_FLEX_VALIDATION
- FND_FORM
- FND_FORM_FUNCTIONS
- FND_GRANTS
- FND_MENUS
- FND_MENU_ENTIRES
- FND_ORACLE_USERID
- FND_PROFILE_OPTIONS

- FND_PROFILE_OPTION_VALUES
- FND_REQUEST_GROUPS
- FND_REQUEST_GROUP_UNITS
- FND_RESP_FUNCTIONS
- FND_USER_RESP_GROUPS

How Data Appears in Tables and View

Here is an example of how data appears in your original table, your shadow table, and your audit views after a series of changes (starting with an empty AUDIT_DEMO table).

```
SQL> INSERT INTO AUDIT_DEMO VALUES (1,'A','A','A');
SQL> INSERT INTO AUDIT_DEMO VALUES (2,'X','X','X');
SQL> SELECT PRIMARY_KEY KEY, VALUE_ONE VAL_1,
     VALUE_TWO VAL_2, VALUE_THREE VAL_3 FROM AUDIT_DEMO;

 KEY VAL_1 VAL_2 VAL_3
---- ----- ----- -----
   1 A     A     A
   2 X     X     X

SQL> UPDATE AUDIT_DEMO SET VALUE_ONE ='B'
     WHERE PRIMARY_KEY = 1;

 KEY VAL_1 VAL_2 VAL_3
---- ----- ----- -----
   1 B     A     A
   2 X     X     X

SQL> UPDATE AUDIT_DEMO SET VALUE_TWO ='B'
     WHERE PRIMARY_KEY = 1;

 KEY VAL_1 VAL_2 VAL_3
---- ----- ----- -----
   1 B     B     A
   2 X     X     X

SQL> UPDATE AUDIT_DEMO SET VALUE_THREE ='B'
     WHERE PRIMARY_KEY = 1;
SQL> UPDATE AUDIT_DEMO SET VALUE_ONE ='Y'
     WHERE PRIMARY_KEY = 2;
SQL> UPDATE AUDIT_DEMO SET VALUE_ONE = NULL
     WHERE PRIMARY_KEY = 1;
SQL> UPDATE AUDIT_DEMO SET VALUE_ONE ='C'
     WHERE PRIMARY_KEY = 1;
```

After our two inserts and six updates, the final values in the audited table are:

```
 KEY VAL_1 VAL_2 VAL_3
---- ----- ----- -----
   1 C     B     B
   2 Y     X     X
```

The final values in the corresponding shadow table are as follows. A row in the shadow table represents the state of the audited row before the audited row was changed. Note

that if a value in a row doesn't change during the transaction, the shadow table records a null for that value in that transaction.

In our example, the first two rows in the shadow table represent the state where there was no data for our two audited rows before they were inserted. The "prior values" are null values for the two insert transaction (type I) rows. Similarly, when we update the first value of row 1 to be the value B instead of A, the shadow table records the value A in its third row:

```
SQL> SELECT TO_CHAR(AUDIT_TIMESTAMP, 'HH24:MI:SS') TIME,
     AUDIT_TRANSACTION_TYPE TYPE, AUDIT_USER_NAME NAME,
     PRIMARY_KEY KEY, VALUE_ONE VAL_1, VALUE_TWO VAL_2,
     VALUE_THREE VAL_3, AUDIT_TRUE_NULLS FROM AUDIT_DEMO_A;

TIME     TYPE NAME    KEY VAL_1 VAL_2 VAL_3 AUDIT_TRUE_NULLS
-------- ---- ------ ---- ----- ----- ----- ----------------
11:08:16 I    FND60     1
11:08:40 I    FND60     2
11:18:40 U    FND60     1 A
11:20:12 U    FND60     1       A
11:21:54 U    FND60     1             A
11:22:15 U    FND60     2 X
14:20:50 U    FND60     1 B
14:21:15 U    FND60     1                   NYNN

8 rows selected.
```

Given the current values of the row in the audited table, you can trace the changes made to the row by backing up through the corresponding rows in the shadow table.

In our example table, we made two insert and six update transactions, so we see those eight transactions in our shadow table. In the last row, the NYNN indicates that the value in the second table column (VALUE_ONE) has changed from an actual null value (the Y) rather than being an unchanged value (represented by null in the shadow table).

The following two views provide further ways of examining your audited data.

The rows with a transaction type of C in the view indicate the current value of the row when the data was selected (the view is a join between the shadow table and the audited table, so the current value row reflects the current state of the audited table).

The _AC view provides a "filled-in" version of the data, where unchanged values appear instead of being represented by null values. You can order this view by the primary key (rather than by timestamp), so all rows in the shadow table that correspond to a single audited row appear together, with a secondary ordering by timestamp.

```
SQL> SELECT TO_CHAR(AUDIT_TIMESTAMP, 'HH24:MI:SS') TIME,
     AUDIT_TRANSACTION_TYPE TYPE, AUDIT_USER_NAME NAME,
     PRIMARY_KEY KEY, VALUE_ONE VAL_1, VALUE_TWO VAL_2,
     VALUE_THREE VAL_3 FROM AUDIT_DEMO_AC1
     ORDER BY PRIMARY_KEY, AUDIT_TIMESTAMP;

TIME     TYPE NAME        KEY VAL_1 VAL_2 VAL_3
-------- ---- ---------- ---- ----- ----- -----
11:08:16 I    FND60         1 A     A     A
11:18:40 U    FND60         1 B     A     A
11:20:12 U    FND60         1 B     B     A
11:21:54 U    FND60         1 B     B     B
14:20:50 U    FND60         1       B     B
14:21:15 U    FND60         1 C     B     B
17:53:34 C                  1 C     B     B
11:08:40 I    FND60         2 X     X     X
11:22:15 U    FND60         2 Y     X     X
17:53:34 C                  2 Y     X     X

10 rows selected.
```

Important: If the changes to your audited table occur faster than one change per second (that is, more frequently than the one-second granularity provided by SYSDATE), you may see "blurring" of records (i.e. more than one record per transaction) in the _AC view, because of joins used in this view. However, the shadow table itself remains correct, and you can resolve the relevant transactions by referring to the shadow table directly.

The _AV1 view provides a more sparse view of the audit data, ordered by timestamp:

```
SQL> SELECT TO_CHAR(AUDIT_TIMESTAMP, 'HH24:MI:SS') TIME,
     AUDIT_TRANSACTION_TYPE TYPE, AUDIT_USER_NAME NAME,
     PRIMARY_KEY KEY, VALUE_ONE VAL_1, VALUE_TWO VAL_2,
     VALUE_THREE VAL_3, AUDIT_TRUE_NULLS
     FROM AUDIT_DEMO_AV1;

TIME     TYPE NAME    KEY VAL_1 VAL_2 VAL_3 AUDIT_TRUE_NULLS
-------- ---- ------ ---- ----- ----- ----- ----------------
11:08:16 I    FND60     1
11:08:40 I    FND60     2
11:18:40 U    FND60     1 A
11:20:12 U    FND60     1       A
11:21:54 U    FND60     1             A
11:22:15 U    FND60     2 X
14:20:50 U    FND60     1 B
14:21:15 U    FND60     1                   NYNN
17:58:31 C              1 C     B     B
17:58:31 C              2 Y     X     X

10 rows selected.
```

Here is an example of how you might use a view to determine who changed a particular value and when:

```
SQL> SELECT TO_CHAR(AUDIT_TIMESTAMP, 'HH24:MI:SS') TIME,
     AUDIT_TRANSACTION_TYPE TYPE, AUDIT_USER_NAME NAME
     FROM AUDIT_DEMO_AV1
     WHERE PRIMARY_KEY = 1
     AND VALUE_ONE = 'B';

TIME     TYPE NAME
-------- ---- ------
14:20:50 U    FND60
```

Similarly, you might want to determine who changed a value to null and when:

```
SQL> SELECT TO_CHAR(AUDIT_TIMESTAMP, 'HH24:MI:SS') TIME,
     AUDIT_TRANSACTION_TYPE TYPE, AUDIT_USER_NAME NAME
     FROM AUDIT_DEMO_AV1
     WHERE PRIMARY_KEY = 1
     AND VALUE_ONE  IS NULL
     AND SUBSTR(AUDIT_TRUE_NULLS,2,1) = 'Y';

TIME     TYPE NAME
-------- ---- ------
14:21:15 U    FND60
```

Reporting on Audit Data

Audit Trail reports are not provided with Oracle E-Business Suite. You may write audit reports as needed using SQL. Audit Trail provides the views of your shadow tables to make audit reporting easier; you can write your reports to use these views.

You may want to create one or more indexes to your shadow table to speed up your reporting. However, such indexes decrease performance during actual auditing of transactions, so you should drop your indexes from the shadow table when you have finished reporting. Another alternative is to move audit data to an operational data store for reporting purposes.

Implications of Upgrading an Audit Trail

> **Important:** Because the structure of the audited table may change between product versions, Audit Trail does not support upgrading existing shadow tables or audited data. Before an upgrade, you should archive the shadow tables and perform all necessary reporting on the audited data.

Auditing database row changes is performance intensive. Limit auditing to non-transactional data. Auditing transactional data may cause significant performance degradation. Tables with more than a few changes an hour should not be considered for row level auditing. Plan and consult with a DBA before enabling Audit Trails.

Disabling Audit Trail

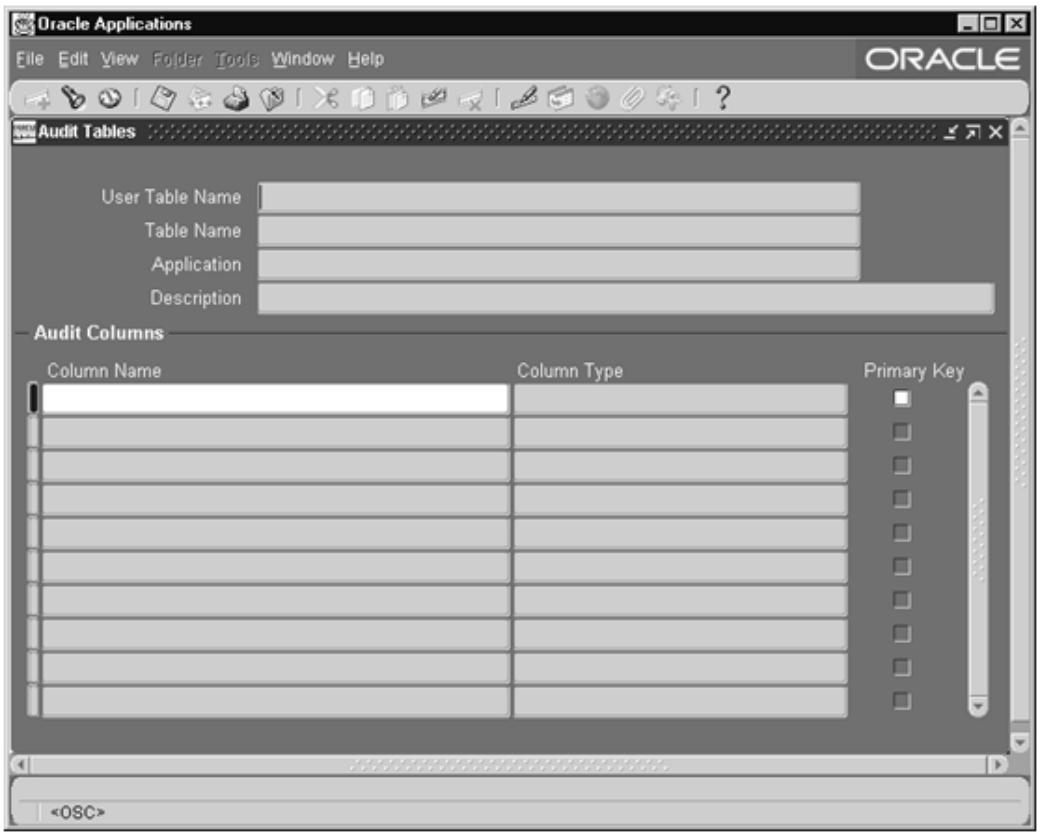
To disable auditing for a group, choose one of the following options and then run the

Audit Trail Update Tables report to have your changes take effect.

Variable Descriptions

Variable	Description
Disable - Prepare for Archive	Copies the current values of all rows in the audited table into the shadow table, and then disables the auditing triggers. This option requires the most space, since there is at least one row in the shadow table for every row in the audited table (and another row in the shadow table for each transaction on the original row in the audited table). You should then archive the table before you empty the shadow table.
Disable - Interrupt Audit	Modifies the triggers to store one final row in the shadow table as the audited row is modified in the audit table (remember that a given row in the shadow table represents the data in the audited row before an update). Inserts or further changes are no longer audited. The shadow table then grows slowly, and the data may be accessed by the existing audit views.
Disable - Purge Table	Drops the auditing triggers and views and deletes all data from the shadow table.

Audit Tables Window



Additional Audit Trail Reporting

This section describes how to set up and manage Audit Trail Reporting functions that are used within OPM.

The following topics are covered:

- Audit Industry Template
- Audit Hierarchy Navigator
- Audit Query Navigator
- Running the Audit Report

Audit Industry Template

This window defines the Audit Industry templates. These templates facilitate binding of the required Audit groups together for easy querying and inquiries.

Before using this window, perform the following:

- Define Audit Tables and Audit columns using Oracle Application Audit under the System Administrator responsibility
- Define Audit Groups using Oracle Application Audit under the System Administrator responsibility

Audit Industry Template Procedure

Use this procedure in completing the Industry Template.

1. Navigate to the **Industry Template** window.
2. Complete the fields as described.
3. Save your changes.

Audit Industry Template Fields

The following are the fields found in the Audit Industry templates.

Audit Industry Template Field Descriptions

Field	Description
Template Name	The name of the desired Audit Template
Functional Areas	Functional Group - Enter the functional group associated with this template. This is the same as the Audit Group field on the Audit Group window in System Administration.

Audit Hierarchy Navigator

Auditing Navigation

In addition to the standard menu and tool bar, a navigator tree provides a hierarchical display of the objects in a treelike framework.

Nodes and Leaves

The higher level nodes in the navigator tree include windows and database objects. All other nodes, and the objects they contain, are indented to indicate that they belong to these higher level nodes. The terminal node is a leaf.

On the Hierarchy Navigator, the highest level is the Audit Template. The next level is the Audit Group (Functional Group), then the audit table, and finally, the columns being audited.

On the Query Navigator, the highest level is the Audit Group (Functional Group). The next level is the audit table, and below the audit table are the actual data being audited.

Using the Audit Hierarchy Editor

You can navigate to find what has been set up for auditing. This functionality is accomplished by a tree navigator that starts with the Industry template and drill down to groups, tables, and columns. The navigator lets you see a drill-down view of what columns are being audited. A search facility on the tree is provided to search a table or column.

The navigator fetches the data from the audit table to construct the tree, and relies on the Oracle E-Business Suite Object Library table, column registration and uses USER_TABLE_NAME and USER_COLUMN_NAME fields from the FND_TABLES and FND_COLUMNS, respectively.

Before using this window, perform the following:

- Define Audit Tables and Audit columns using the Oracle Application Audit under the System Administrator responsibility
- Define Audit Groups using Oracle Application Audit under the System Administrator responsibility
- Define Industry Audit Templates under the OPM System Administrator responsibility
- Enable Audit Trail, a concurrent process under the System Administrator responsibility

Audit Hierarchy Navigation Procedures

Navigate to the Audit Hierarchy window.

To view table information:

1. Use the tree navigator to view the table names.
2. Select the table name and right-click to display the pop-up menu.
3. Select **Display Columns**. The Define Query Navigator Display for the Table window appears.

To use the Find Audit Hierarchy function:

1. Use the tree navigator to view the column names.

2. Select the column name and right-click to display the pop-up menu.

3. Select Find. The Find Audit Hierarchy window displays.

4. Select criteria and click Find. A list of templates displays. You can save these as a new audit.

Audit Query Navigator

This interactive query window lets you investigate the changes to any functional group interactively, using a visual approach that is similar to Windows Explorer. When a particular node in the left frame is selected, audit trail details are displayed in the right frame. The right frame shows all columns set for auditing. This information is retrieved from the FND_AUDIT_COLUMNS table. The left tree is linked to the right frame with the primary key combination of the table.

Auditing Navigation

In addition to the standard menu and tool bar, a navigator tree provides a hierarchical display of the objects in a treelike framework.

Nodes and Leaves

The higher level nodes in the navigator tree include windows and database objects. All other nodes, and the objects they contain, are indented to indicate that they belong to these higher level nodes. The terminal node is a leaf.

On the Hierarchy Navigator, the highest level is the Audit Template. The next level is the Audit Group (Functional Group), then the audit table, and finally the columns being audited.

On the Query Navigator, the highest level is the Audit Group (Functional Group). The next level is the audit table, and below the audit table are the actual data being audited.

Before using this window, perform the following:

- Define Audit Tables and Audit columns using the Oracle Application Audit under the System Administrator responsibility.
- Define Audit Groups using Oracle Application Audit under the System Administrator responsibility.
- Define Industry Audit Templates under the OPM System Administrator responsibility.
- Define the display look up using the Audit Hierarchy Navigator (Admin Mode). This setup step is not mandatory.
- Enable Audit Trail, a concurrent process under the System Administrator

responsibility.

Audit Query Navigation Procedures

Navigate to the Audit Query window.

To use the Find Functional Groups function:

1. Use the tree navigator to view the tables names.
2. Select the table name and right-click to display the pop-up menu.
3. Select **Find**. The Find Function Groups window displays.
4. Select criteria and click **Find**. A list of templates displays. You can save these as a new audit.

To view the Audit Results window:

1. Use the tree navigator to view the column names.
2. Select a column name. The Audit Results window automatically displays.
3. Use the Horizontal View and Vertical View buttons to toggle between the two views.

   In the horizontal view, you see the first ten auditing columns. In the vertical view, the column number is unlimited and can be viewed using the scroll bar.

Audit Report

In situations where comprehensive documentation is needed (such as to support legal or regulatory requirements), a single report request resulting in a single comprehensive report is desirable. This report can then be printed, sent by email, or archived.

Since this report could involve a considerable amount of data, a detailed parameter screen is available, allowing you to select only the items of interest.

Submitting the Report

1. Navigate to the Audit Report window. The Enter Report Parameters window is displayed.
2. Select the functional group, or a functional group and audit table name.
3. Complete the optional fields as necessary.
4. Click **Select Columns**. The Select Reporting Columns window is displayed.

5. Enter at least one column to run the report. The columns displayed are based on the functional group, or a functional group and audit table name criteria selected on the Enter Report Parameters window.

6. Select **Print Options**. The Select Printing Options window is displayed.

7. Enter the necessary print information.

8. Click **OK**.

9. Run the report by selecting **Run Report**.

Enter Report Parameters Field Reference

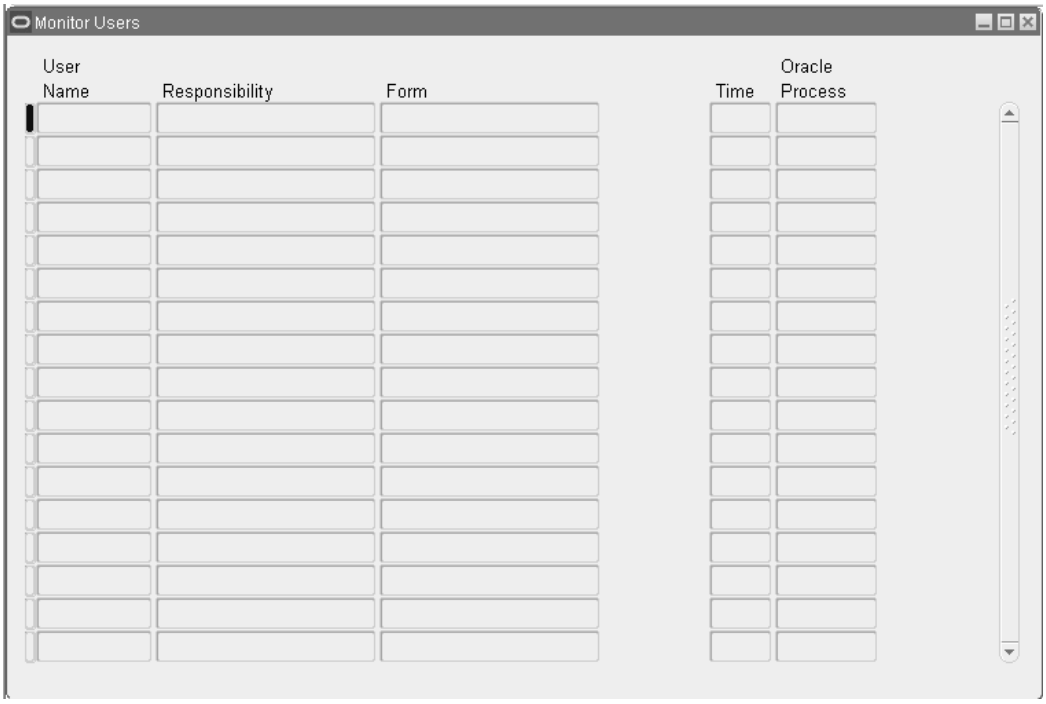
Report Parameters Field Descriptions

Field	Description
Functional Group	Specify the name of the functional group for the report. This is the same as the Audit Group field on the Audit Group window in System Administration.
Audit Table Name	Optional. Specify the table name from the functional group for the report.
Transacted By	Optional. Specify the user who is requesting the report.
Transaction Type	Optional. Specify the type of transaction.
From Date	Optional. Specify the beginning date for the date range the report will run.
To Date	Optional. Specify the end date for the date range the report will run.

Monitor Users Window

Use this window to monitor what your application users are currently doing.

Monitor Users Window



As well as seeing which users are signed on, you can see:

- Which responsibilities and forms (windows) they are using.
- How long they have been logged in.
- What Oracle database processes they are using.
- The client server's IP address.

In addition, you can monitor all users at a site, all users accessing a specific application, or a specific responsibility, or individual users.

> **Note:** You can only monitor those users for whom you have activated Sign-On Audit. See: Enabling Sign-On Audit, page 16-4.

Before using this form, select a value for the Sign-On:Audit Level profile option, using the Update System Profile Options Window.

To access, navigate to **System Administration**, and then **User Monitor**.

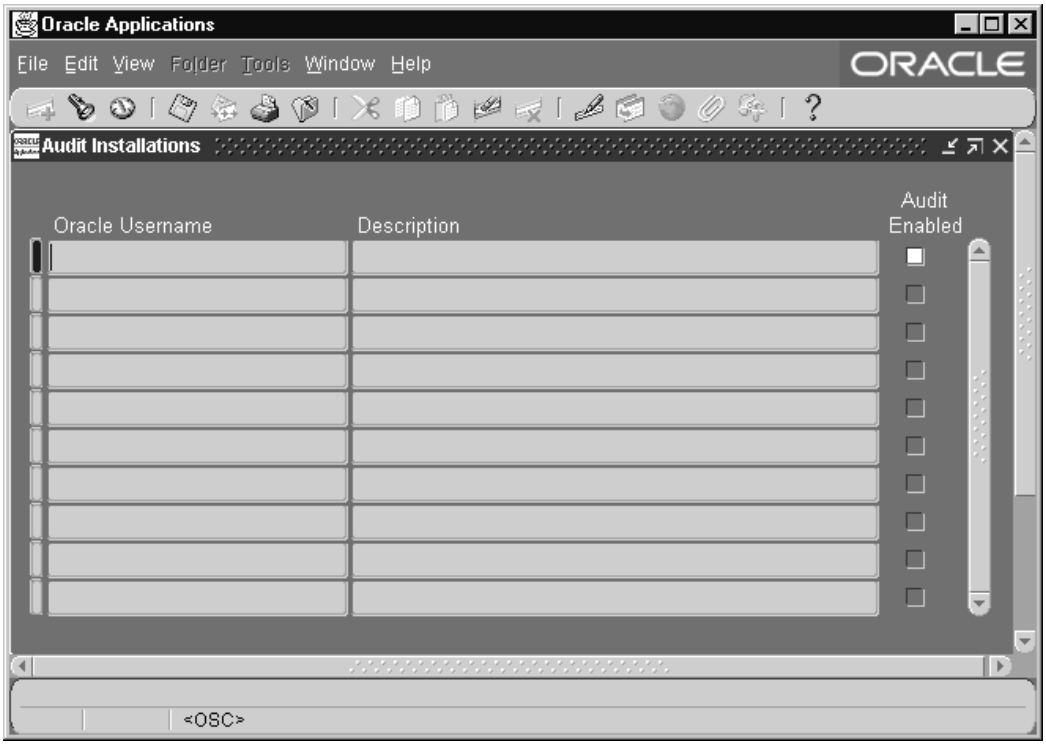
Monitor Users Window Field Descriptions

Field	Description
User Name	The user's login name.
Responsibility	The user's responsibility only appears if you have enabled Sign-On Audit at either the Responsibility or Form audit level.
Form	The user's form only appears if you have enabled Sign-On Audit at the Form audit level.
Time	The length of time the user has been logged on to this application.
Process	The ORACLE process of the user.
Client IP Address	The IP address of the client server.

Audit Installations Window

Use this window to enable Audit Trail for an Oracle database user name at your installation. Such a user name grants access privileges to an application's tables and database objects.

Audit Installations Window



For auditing to take effect, you must also define one or more audit groups and run the Audit Trail Update Tables report. See: Reporting on Audit Trail Data.

Before using this form, ensure that the desired Oracle user name is registered. The installation process automatically registers Oracle E-Business Suite Oracle user names, but if you create a custom application, you should follow the instructions in My Oracle Support Knowledge Document 1577707.1, *Creating a Custom Application in Oracle E-Business Suite Release 12.2*, for Oracle user names for custom applications.

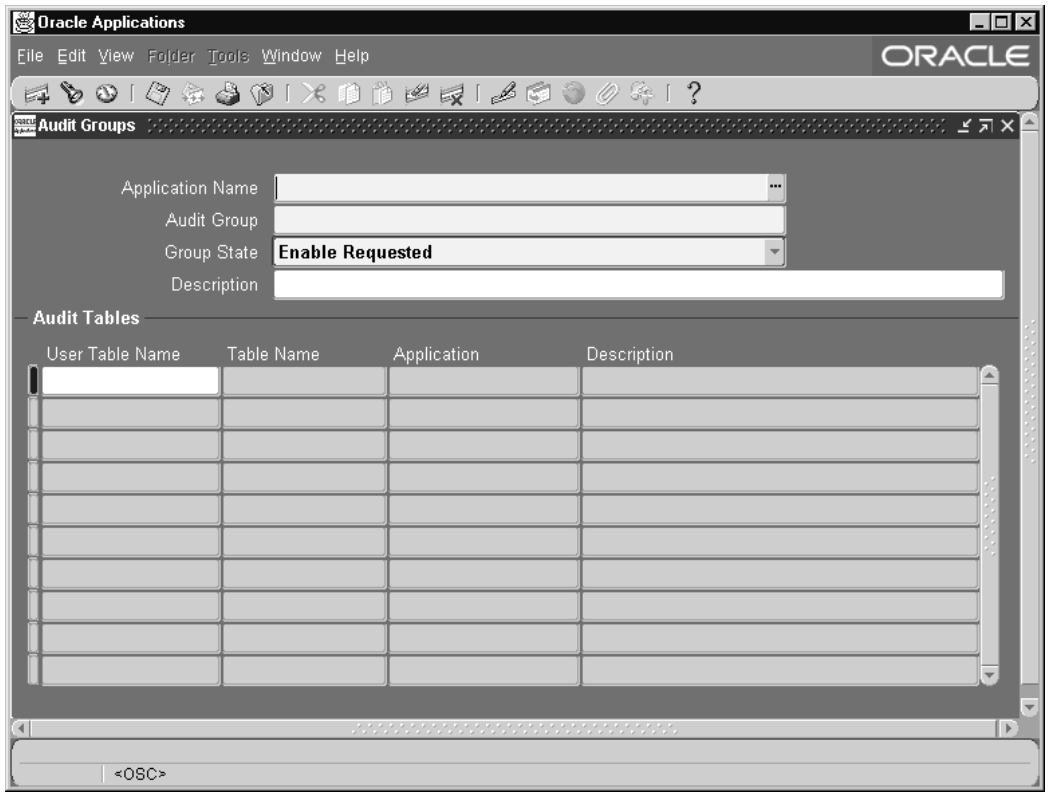
Audit Installations Window Element Descriptions

Element	Description
Oracle Username	Select the Oracle user name that owns the tables you wish to audit.
Audit Enabled	Select the Audit Enabled checkbox to enable Audit Trail for an Oracle user name. Before auditing takes effect, you must define one or more audit groups and run the Audit Trail Update Tables report.

Audit Groups Window

Use this window to select the tables that you wish to audit. You audit a table by defining an audit group, which can consist of one or more tables.

Audit Groups Window



First, identify the tables you want to audit. Then, using the Audit Tables window, select which columns in each table you wish to audit. Or, select which columns in a particular table you wish to audit (using the Audit Tables window), then define your audit group (using this window).

To enable or disable auditing for the tables in your audit group, run the Audit Trail Update Tables program using the Submit Requests window. If you change the definition or audit state of your group later, you must rerun this program.

Before defining your audit groups, make sure you have defined an audit installation using the Audit Installations window.

> **Note:** Your tables and their primary key information must already be registered and defined for successful auditing. If the table you want to audit is a custom table (not shipped as part of Oracle E-Business Suite),

you should also perform the following two steps:

- Register your table *and* its primary key columns using Oracle Application Object Library's Tables window (Application Developer Responsibility).
- Run the Register Tables concurrent program from the Submit Requests window.

Audit Groups Block

Identify your audit group and enable or disable auditing for this group.

Application Name

Select the name of an application to associate with your audit group. The combination of application name and group name uniquely identifies your audit group. An audit group may be used to audit tables in additional applications.

Audit Group

Enter the name of the audit group.

Group State

Choose Enable Requested if you are defining a new audit group. When you run the Audit Trail Update Tables report, the concurrent program creates database triggers for the tables in your audit group. Once you have run the program, this field displays Enabled for audit groups where AuditTrail is active.

> **Important:** All primary key columns in each table in an audit group are automatically selected for auditing, whether or not you use the Audit Tables window to select which columns you wish to audit.

To disable auditing for a group, choose one of the following options and then run the Audit Trail Update Tables report to have your changes take effect.

Disable - Prepare for Archive
Copies the current values of all rows in the audited table into the shadow table, and then disables the auditing triggers. This option requires the most space, since there is at least one row in the shadow table for every row in the audited table (and another row in the shadow table for each transaction on the original row in the audited table). You should then archive the table before you empty the shadow table.

Disable - Interrupt Audit

Modifies the triggers to store one final row in the shadow table as the audited row is modified in the audit table (remember that a given row in the shadow table represents the data in the audited row *before* an update). Inserts or further changes are no longer audited. The shadow table then grows slowly, and the data may be accessed by the existing audit views.

Disable - Purge Table

Drops the auditing triggers and views and deletes all data from the shadow table.

Audit Tables Block

Identify the application tables you want to audit in your audit group.

User Table Name

Select the end user table name (frequently the same name as the table name) for your database table. Once you choose a table, you see its table name and associated application.

Table Name

This field displays the actual name for the table you have selected to include in your audit group.

Application

This field displays the application name for the table you have selected to include in your audit group.

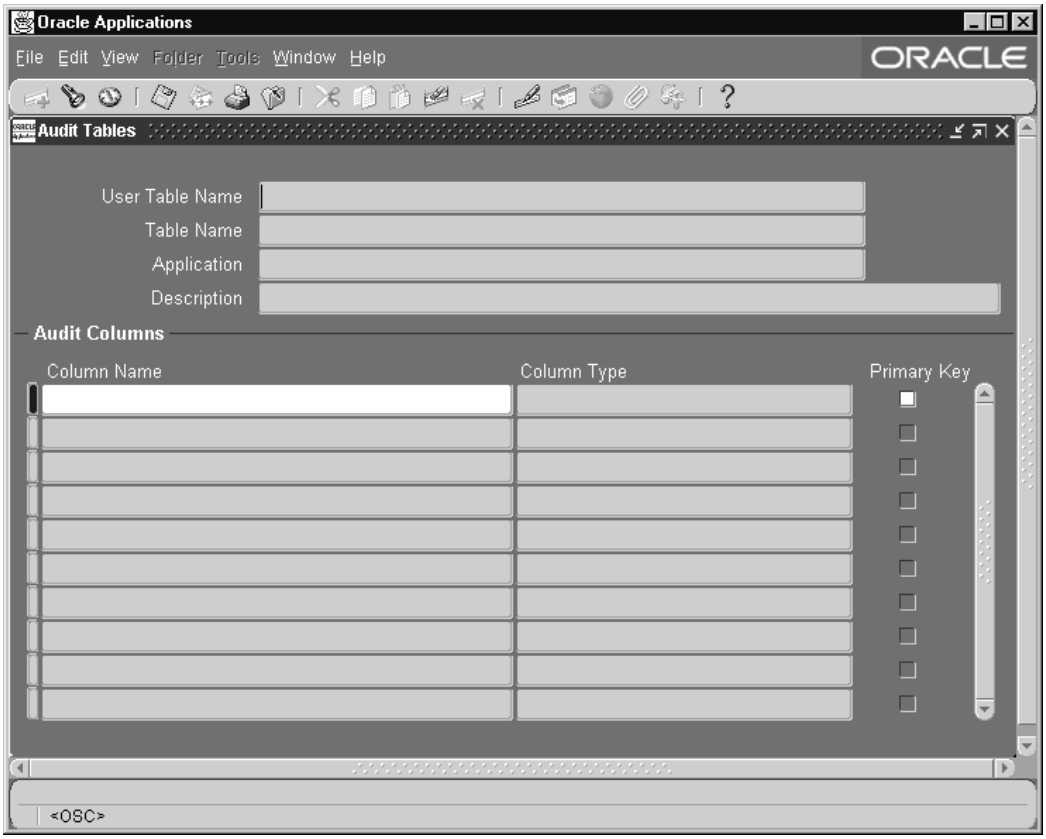
Description

This field displays the description for the table you have selected to include in your audit group.

Audit Tables Window

Use this window to select which columns in a table you wish to audit.

Audit Tables Window



First, identify the columns in a table you want to audit. Then, using the Audit Groups window, include the table as part of an audit group. Or, you may define your audit group first (using the Audit Groups window), and then select which columns in the table you want to audit (using this window).

To enable or disable auditing for the tables in your audit group (i.e., the columns you have selected here), you must run the Audit Trail Update Tables program using the Submit Requests window. If you select additional columns to audit, or change the definition or audit state of your group later, you must rerun this program.

Before defining your audit tables, make sure that you have defined an audit installation using the Audit Installations window.

> **Important:** Your tables and their primary key information must already be registered and defined for successful auditing. If the table you want to audit is a custom table (not shipped as part of Oracle E-Business Suite), you should also perform the following two steps:
>
> - Register your table and its primary key columns using Oracle Application Object Library's Table window (Application Developer

Responsibility).

- Run the Register Tables concurrent program from the Submit Requests window.

Define Audit Tables Block

Identify the application table you want to audit. Successively selecting *Go - Next Record* from the menu or toolbar displays, in alphabetical order, the name of each application table registered at your installation site.

User Table Name

Select the end user table name (frequently the same name as the table name) for your database table. Once you choose a table, you see its table name and associated application.

Table Name

This field displays the actual name for the table you have selected to include in your audit group.

Application

This field displays the application name for the table you have selected to include in your audit group.

Audit Columns Block

Select the columns you want to audit. Successively selecting *Go - Next Record* from the menu or toolbar displays, in alphabetical order, the name of each application table registered at your installation site.

- You cannot delete a column from auditing once it has been selected.
- You may add additional columns to be audited.
- Each time you select a column to be audited, that change affects every audit group that includes the table which owns the column.

Column Name

Enter the name of the database column you want to audit. You should not explicitly enter the names of your table's primary key columns, since they are entered automatically, and you will get an error message if you try to save a duplicate column name. You can query to see which columns appear automatically.

Note that once you have chosen a column, you cannot delete it from the audit set, though you may add other columns to the set later.

Once you choose a column, you see its column type and whether it is part of the primary key for this table.

Column Type

This field describes the type of data the column stores, for example, varchar2.

Primary Key

This field displays Yes or No indicating whether the column you are auditing is a primary key column.

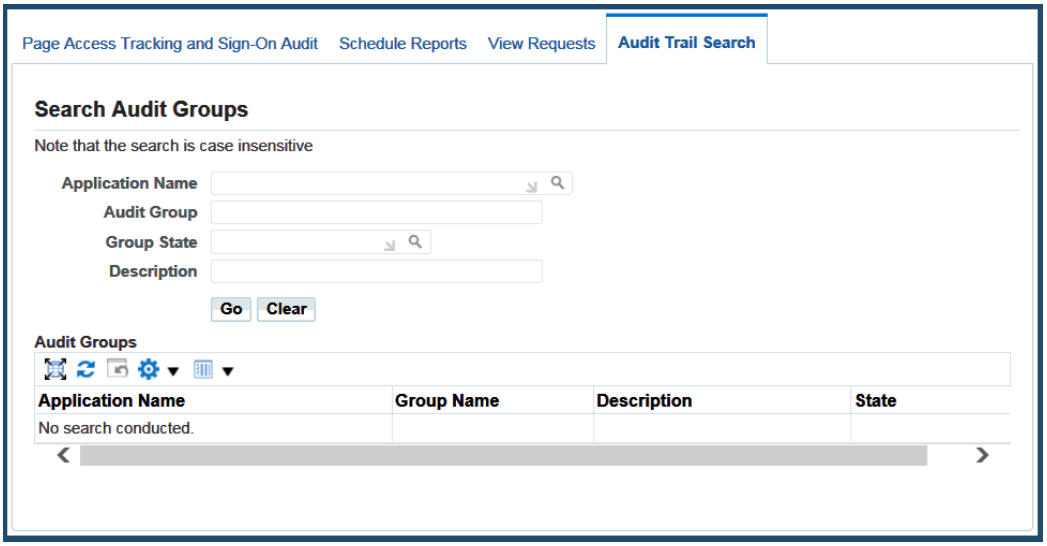
Any primary key columns you do not select to audit are automatically included when you save your column selections. For example, if the table you are auditing has two primary key columns, and you choose to audit one of them, the second primary key column is automatically selected when you save your column selections.

Audit Trail Search Pages

The Audit Trail Search pages allow you to query audit trail setup tables without launching the Forms-based Audit Trail windows.

You can navigate to these pages from the Auditing Manager responsibility. Choose Audit Trail Search from the menu.

Audit Trail Search Page



Search Audit Groups

You can search on any of the following criteria:

- Application Name
- Audit Group
- Group State
- Description

The search will retrieve the Master Record from the FND_AUDIT_GROUPS table; all audit groups that satisfy your search criteria will be returned.

In the Audit Groups search results table, the Group Name for each record is a link. This link allows you to get the rest of the details for the particular audit group.

Audit Group

This page lists the audit tables that are defined for the audit group. For each table, the following is shown:

- User Table Name
- Table Name (link)
- Application Name

- Description

Clicking on the Table Name link allows you to drill down for more information on that table.

Audit Table

This page lists the columns that are being audited for a particular table.

For each column, the Column Name and Column Type is listed.

A

Running Web Scanning Tools

Overview

Over the years, Oracle has run web scanning tools such as AppScan and WebInspect against Oracle E-Business Suite and a number of our customers have also submitted reports generated by these tools.

In this section we will share some of the experience we have gained through this process.

Preparing Your Oracle E-Business Suite System for the Web Scan

To get the best value of the effort you invest in the pen test, you should first secure your Oracle E-Business Suite instance as described in this document. In particular, you should ensure that the security settings that directly affect the web interface are set properly.

Refer to the following table and set the recommended values for the profile options.

Suggested Profile Option Values for Preparing Your Oracle E-Business Suite System for the Web Scan

Profile Option Name	Code (Internal Name)	Recommended Value
Utilities:Diagnostics	DIAGNOSTICS	No
FND: Diagnostics	FND_DIAGNOSTICS	No
Restrict Text Input	FND_RESTRICT_INPUT	Y

Profile Option Name	Code (Internal Name)	Recommended Value
Attachment File Upload Restriction Default	FND_SECURITY_FILETYPE_ RESTRICT _DFLT	Y
FND: Disable Antisamy Filter	FND_DISABLE_ANTISAMY_ FILTER	No

My Oracle Support Knowledge Document 946372.1, *Secure Configuration of E-Business Suite Profiles* [https://support.oracle.com/rs?type=doc&id=946372.1], describes the Diagnostics and Validation profiles in more detail.

FND_DIAGNOSTICS=N

If you set diagnostics to "Yes", you will receive numerous reported issues concerning "Information Leakage." This is because when in diagnostics mode, Oracle E-Business Suite will return stack traces to the client to help in diagnosing problems.

FND_RESTRICT_INPUT=Y

Setting this to "Y" activates the input scanner; the input scanner will check the input parameters for common malicious patterns and block the request if any are found.

FND_SECURITY_FILETYPE_RESTRICT_DFLT=N

Setting this to "N" enables an allowlist of authorized file extensions, rather than the default blocklist specified by "Y."

Reviewing the Results

The web scanning tool attempt to find vulnerabilities of various types. In our experience the web-scanning tools excel at finding certain types of vulnerabilities and have less success with other types.

Reflected XSS and Header Splitting

The tools are generally very good at finding these types of vulnerabilities and most reported issues are actual issues.

Stored XSS

Finding these are much harder and generally the accuracy is lower than for Reflected XSS.

In the few cases we have seen the 'stored' claim was based on tainted input being carried between pages in a page flow, not necessarily in an 'executable page context' and certainly not stored in the database.

SQL-Injection

Tools tend to produce a high proportion of false positive for SQL Injections.

The most common reason for reported 'potential SQL Injections' is that the tool recognizes a database error code in the response and concludes that there might be a 'potential SQL Injection'.

The most common source of these 'database errors' is:

- PL/SQL data type validation errors
- JDBC connect errors

PL/SQL errors typically come from calling java or jsp URLs that call PLSQL APIs.

In this case, the server-side code is executing in the database and any error reported is likely to be "a database error." Typical errors are plsql data validation errors such as "buffer too small" and "that's not an integer" of the ORA-06502 family. Another source of error is "that string cannot be decoded", seen when messing with submitted cookie values.

These PL/SQL errors may be indicative of "Information Leakage" but they are not SQL Injections.

- ORA-06502: PL/SQL: character string buffer too small
- ORA-06502: PL/SQL: numeric or value error: number precision too large
- ORA-06502: PL/SQL: numeric or value error: hex to raw conversion error

The JDBC connection errors are seen when the web scanning tool overwhelms the tested instance with a rapid fire of requests. In some cases the connection pool between the application tier and the database gets exhausted and no more database connections can be made. In this situation JDBC errors such as "read() returned -1" are thrown indicating that a database connection could not be made.

These errors may trigger the tool to report "potential SQL Injection" issues as the error stack includes reference to jdbc. Again a potential case of "Information Leakage" but not a SQL injection.

Sample Code Installed

Oc4j, which is the servlet container used in Release 12.0 and 12.1, has the unusual feature that it just cannot say "no."

When it receives a request for a file that does not exist, it will always respond with a "200 OK" response with no content - the tool may have expected a "`404 Not Found`."

Web scanning tools that rely solely on the response status code will think that the file exists and not notice that there is no content served. This may cause the tool to report

the presence of "Sample Code," "Known Bad files," or "Alternate Version of File" when no such files exist.

Note that "no content" may be indicated by a Content-Length: 0 header or if the `Transfer-Encoding: chunked` header is present the size of the first and only chunk will be 0.

B

Database Schemas Found in Oracle E-Business Suite

This appendix covers the following topics:

- Table of Database Schemas in Oracle E-Business Suite

Table of Database Schemas in Oracle E-Business Suite

Type	Schemas	Change	Managed	Description
1	SYS	Y	N	Initial schema in any Oracle database. Owns the SQL data dictionary. This account is used to grant privileges to EBS_SYSTEM. After the EBS System Schema Migration Completion patch, this account is no longer required for Oracle E-Business Suite administration.

Type	Schemas	Change	Managed	Description
1	SYSTEM	Y	N	Initial DBA User. After the EBS System Schema Migration Completion patch, this account is no longer required for Oracle E-Business Suite administration.
1	EBS_SYSTEM	Y	N	With AD-TXK Delta 13, this account is the Applications DBA system administration account. After the EBS System Schema Completion patch, this account is the only account required to perform Oracle E-Business Suite administration.
1	DBSNMP SYSMAN MGMT_VIEW	Y	N	Used for database status monitoring.
2	SCOTT	Y	N	Demo account delivered with RDBMS.
2	SSOSDK	Y	N	Single Sign On SDK.

Type	Schemas	Change	Managed	Description
3	JUNK_PS MDSYS ODM_MTR OLAPSYS ORDPLUGINS ORDSYS OUTLN OWAPUB MGDSYS	Y	N	
3	PORTAL30_DEMO PORTAL30_PUBLIC PORTAL30_PS PORTAL30_SSO_PUBLIC	Y	N	Oracle Portal and Portal Single Sign On
4	PORTAL30 PORTAL30_SSO	Y	Y	Oracle Portal and Portal Single Sign On
4	CTXSYS	Y	Y	Oracle Multimedia (formerly *inter* Media) schema used by Online Help and CRM service products for indexing knowledge base data.
4	EDWREP	Y	Y	Embedded Data Warehouse Metadata Repository
4	ODM	Y	Y	Oracle Data Manager

Type	Schemas	Change	Managed	Description
5	APPLSYSPUB	Y	Y	Initial, pre-authentication user with minimal privileges to assist with APPS (FND) user authentication.
5	APPLSYS	Y	Y	Contains shared APPS objects.
5	APPS APPS_NE	Y	Y	Runtime user for E-Business Suite. Owns all of the applications code in the database. (APPS_NE is new in R12.2)
5	APPS_mrc	Y	Y	Optional, additional APPS schemas for the (now obsolete) Multiple Reporting Currencies feature. Defaults to APPS_MRC, but country code suffixes may be used, e.g. APPS_UK, APPS_JP.
5	AD_MONITOR EM_MONITOR	Y	N	Used by Oracle Applications Manager (OAM) or EM to monitor patching.

Type	Schemas	Change	Managed	Description
6	ABM AHL AHM AK ALR AMF AMS AMV AMW AP AR ASF ASG ASL ASN ASO ASP AST AX AZ BEN BIC BIL BIM BIS BIV BIX BNE BOM BSC CCT CE CLN CN CRP CS CSC CSD CSE CSF CSI CSL CSM CSP CSR CSS CUA CUE CUF CUG CUI CUN CUP CUS CZ DDD DDR DNA DOM DPP EAA EAM EC ECX EDR EGO ENG ENI EVM FA FEM FII FLM FPA FPT FRM FTE FTP FUN FV GCS GHG GL GMA GMD GME GMF GMI GML GMO GMP GMS GR HR HRI HXC HXT IA IBA IBC IBE IBP IBU IBW IBY ICX IEB IEC IEM IEO IES IEU IEX IGC IGF IGI IGS IGW IMC IMT INL INV IPA IPD IPM ISC ITA ITG IZU JA JE JG JL JMF JTF JTM JTS LNS ME MFG MRP MSC MSD MSO MSR MST MTH	Y	Y	These schemas belong to individual APPS base products. By default the password is the same as the SCHEMA name. Changing the password for these schemas does not affect any configuration files.

Type	Schemas	Change	Managed	Description
	MWA OE OKB OKC OKE OKI OKL OKO OKR OKS OKX ONT OPI OSM OTA OZF OZP OZS PA PFT PJI PJM PMI PN PO POA POM PON POS PRP PSA PSB PSP PV QA QOT QP QPR QRM RG RHX RLA RLM RRS SSP VEA VEH WIP WMS WPS WSH WSM XDO XDP XLA XLE XNB XNC XNI XNM XNP XNS XTR ZFA ZPB ZSA ZX			

In the previous table, "Type" refers to the categories listed in Change Default Installation Passwords, page 8-2. Change means we recommend changing the default password for the listed schemas. Managed means that AFPASSWD (or FNDCPASS) should be used to change the passwords of the listed schemas.

You can identify Oracle E-Business Suite managed schemas by querying the table FND_ORACLE_USERID. The managed schemas are all listed in FND_ORACLE_USERID. The READ_ONLY_FLAG identifies the category.

- C - Category 5 - APPLSYSPUB
- U - Category 5 - APPS
- E - Category 5 - APPLSYS and APPS_NE
- U - Category 5 - APPS variations for the obsolete Multiple Reporting Currencies feature
- A - Category 6 - Oracle E-Business Suite Base Product schemas
- X - Category 4 - Non-Oracle E-Business Suite schemas

Of the two commands to change a managed password, AFPASSWD is the newest and

more compliant with security best practice. It is available as of Oracle E-Business Suite Release 12.1.3. AFPASSWD is documented in the *Oracle E-Business Suite Maintenance Guide*.

In the examples below, we use FNDCPASS syntax as these can be shown on a single line.

For troubleshooting issues with running FNDCPASS, see My Oracle Support Knowledge Document 1306938.1, *FNDCPASS Troubleshooting Guide For Login and Changing Applications Passwords*.

Note, SQL*Plus provides two methods to change a schema's password: ALTER USER and PASSWORD syntax. To simplify these instructions, we have used the ALTER USER syntax. However, PASSWORD is often mentioned as the preferred method for changing a schema's password due to the lack of an echo back to the terminal.

The syntax for changing a schema password from within SQL*Plus is:

```
SQL> password <account>
Changing password for <account>
New password: <new-password>
Retype new password: <new-password>
```

Category 1 - SYS

Change the password for this schema:

```
SQL> alter user SYS identified by <NEW_SYS_PASSWORD>;
```

Category 1 - EBS_SYSTEM & SYSTEM

Password handling for these schemas depends on your codelevel.

- If your instance is on AD-TXK Delta 13 or later and you have not applied the EBS System Schema Migration Completion patch, then the passwords for EBS_SYSTEM and SYSTEM must match. You can use the utility `adValidateEbssystemSchema.pl` to check if the SYSTEM and EBS_SYSTEM passwords match.

- If your instance is on AD-TXK Delta 13 or later and you have applied the EBS System Schema Migration Completion patch, then the EBS_SYSTEM and SYSTEM passwords should be unique.

- If you are on an earlier AD-TXK RUP, then your instance does not have the EBS_SYSTEM account.

The passwords for EBS_SYSTEM and SYSTEM can be modified as follows:

```
SQL> alter user SYSTEM identified by <NEW_SYSTEM_PASSWORD>;
SQL> alter user EBS_SYSTEM identified by <NEW_EBS_SYSTEM_PASSWORD>;
```

Category 1 - DBSNMP, SYSMAN & MGMT_VIEW

These schemas are used by Oracle Enterprise Manager. The Enterprise Manager agent connects to DBSNMP for monitoring and management purposes. The Enterprise Manager application connects to SYSMAN. If you are not using Enterprise Manager with your applications database, follow database instructions for managing this account. If you are using Oracle Enterprise Manager with your applications database, you should change the password for these schemas using sqlplus and configure/re-configure Enterprise Manager accordingly. Instructions to do this are dependent on the version of Oracle Enterprise Manager in use.

Category 2 - SCOTT & SSOSDK

Change the password for SSOSDK:

```
SQL> alter user SSOSDK identified by <NEW_SSOSDK_PASSWORD>;
```

Lock the SCOTT schema:

```
SQL> alter user SCOTT account LOCK;
```

Category 3 - JUNK_PS, MDSYS, ODM_MTR, OLAPSYS, ORDPLUGINS, ORDSYS, OUTLN, OWAPUB, MGDSYS

Change the passwords for these schemas:

```
SQL> alter user <SCHEMA> identified by <NEW_PASSWORD_FOR_SCHEMA>;
```

Category 3 - PORTAL30_DEMO, PORTAL30_PUBLIC, PORTAL30_SSO_PS & PORTAL30_SSO_PUBLIC

If you are using Oracle Login Server and Portal 3.0.9 with Oracle E-Business Suite Release 11i as documented in My Oracle Support Knowledge Document 146469.1, *Configuring Oracle Applications 11i With Oracle Portal*, you should change the passwords for PORTAL30_PUBLIC, PORTAL30_SSO_PS & PORTAL30_SSO_PUBLIC and lock the PORTAL30_DEMO schema:

```
SQL> alter user PORTAL30_DEMO account lock;
SQL> alter user PORTAL30_PUBLIC identified by <newpassword>;
SQL> alter user PORTAL30_SSO_PS identified by <newpassword>;
SQL> alter user PORTAL30_SSO_PUBLIC identified by <newpassword>;
```

If you are not using Oracle Login Server and Portal 3.0.9 with Oracle E-Business Suite Release 11i as documented in My Oracle Support Knowledge Document 146469.1, *Configuring Oracle Applications 11i With Oracle Portal*, then log into SQL*Plus with administrative privileges and lock these schema:

```
SQL> alter user PORTAL30_DEMO account lock;
SQL> alter user PORTAL30_PUBLIC account lock;
SQL> alter user PORTAL30_SSO_PS account lock;
SQL> alter user PORTAL30_SSO_PUBLIC account lock;
```

Alternatively, if you are not using any PORTAL30 integration, you may remove the

PORTAL30% schemas by following instructions in My Oracle Support Knowledge Document 312349.1, *How to Remove Oracle Portal 3.0.9 from E-Business Suite 11i*.

Category 4 - PORTAL30 & PORTAL30_SSO

If you are using Oracle Login Server and Portal 3.0.9 with Oracle E-Business Suite Release 11i as documented in My Oracle Support Knowledge Document 146469.1, *Configuring Oracle Applications 11i With Oracle Portal*, you must use FNDCPASS to change the PORTAL30 and PORTAL30_SSO passwords

```
$ FNDCPASS APPS/<apps_pwd> 0 Y SYSTEM/<system_pwd> ORACLE PORTAL30 <new
pwd>
$ FNDCPASS APPS/<apps_pwd> 0 Y SYSTEM/<system_pwd> ORACLE PORTAL30_SSO
<new_pwd>
```

After you change the PORTAL30 and PORTAL30_SSO passwords, run AutoConfig as documented in My Oracle Support Knowledge Document 165195.1, *Using AutoConfig to Manage System Configurations with Oracle Applications 11i*. For more information, refer to My Oracle Support Knowledge Document 146469.1, *Configuring Oracle Applications 11i With Oracle Portal*, which describes the Portal 3.0.9 installation.

If you are not using Oracle Login Server and Portal 3.0.9 with Oracle E-Business Suite Release 11i as documented in My Oracle Support Knowledge Document 146469.1, *Configuring Oracle Applications 11i With Oracle Portal*, then log into SQL*Plus with administrative privileges and lock these schema:

```
SQL> alter user PORTAL30 account lock;
SQL> alter user PORTAL30_SSO account lock;
```

Alternatively, if you are not using any PORTAL30 integration, you may remove the PORTAL30% schemas by following instructions in My Oracle Support Knowledge Document 312349.1, *How to Remove Oracle Portal 3.0.9 from E-Business Suite 11i*.

Category 4 - EDWREP & ODM

Use FNDCPASS to change the password for these schemas:

```
$ FNDCPASS APPS/<apps_pwd> 0 Y SYSTEM/<system_pwd> ORACLE <schema>
<new_pwd>
```

If not using Embedded Data Warehouse, lock and expire EDWREP schema.

Category 4 - CTXSYS

Oracle E-Business Suite uses the CTXSYS schema.

For non-multitenant databases, the CTXSYS password should be changed to a non-default value using FNDCPASS.

For multitenant databases, the CTXSYS password must be changed within the CDB$ROOT container using the CONTAINER=ALL clause, as follows:

```
SQL> alter user CTXSYS identified by <newpassword> CONTAINER=ALL;
```

Category 5 - APPLSYS, APPS, APPS_NE & APPS_MRC

APPLSYS, APPS (and APPS_NE in R12.2) and any additional APPS_mrc schemas share the same password. APPS is the shared runtime schema for all Oracle E-Business Suite products. APPS_MRC is an obsolete account, although it may be used in older versions of Oracle E-Business Suite. FNDCPASS knows the password must be synchronized across these schemas. Use a long (12 or more characters), secure password for these schemas.

```
$ FNDCPASS APPS/<apps_pwd> 0 Y SYSTEM/<system_pwd> SYSTEM APPLSYS
<new_pwd>
```

After changing the shared password for these schemas you must run AutoConfig to propagate the changed passwords into the application server configuration files.

All application tier processes (apaches, ccm, forms server) must be restarted following the password change and password propagation.

Category 5 - APPLSYSPUB

APPLSYSPUB schema has sufficient privileges to perform the authentication of an Applications User (also known as FND user), which includes running PL/SQL packages to verify the user name/password combination and the privilege to record the success or failure of a login attempt.

If you choose to change this password, you must use FNDCPASS and run AutoConfig to propagate the change to application tier configuration files.

Before running AutoConfig, update the `s_gwyuid_pass` and `s_gwyuid` variables with the new password in the AutoConfig context file:

```
$ vi $CONTEXT_FILE
```

Note that the APPLSYSPUB password must be uppercase, even if case sensitive passwords have been turned on in your Oracle Database 11g or later (SEC_CASE_SENSITIVE_LOGON=true).

```
$ FNDCPASS APPS/<apps_pwd> 0 Y SYSTEM/<system_pwd> ORACLE APPLSYSPUB
<new_pwd>
```

All application tier processes must be restarted following the password change and password propagation.

Category 5 - AD_MONITOR

Oracle Applications Manager uses this schema to monitor running patches. Although the default password for AD_MONITOR is 'lizard', the schema is shipped locked and expired.

The SQL script `$AD_TOP/patch/115/sql/admonusr.sql` creates AD_MONITOR.

Category 6 - ABM ... ZX

Change all of these product schema passwords. For more information, see Change Default Installation Passwords, page 8-2.

If after running this `ALLORACLE` command you are still left with some schemas with unchanged password the reason may be that the schema is no longer "registered" as an Oracle E-Business Suite schema in FND_ORACLE_USERID. If this is the case, then the Oracle E-Business Suite password utility (AFPASSWD or FNDCPASS) will not change the password. You will need to use the Oracle Database SQL command `ALTER USER` to change any remaining schema passwords that still have default values.

This can happen for the following schemas: IBA IMT IPD OKB OKO OKR ABMAHM VEH XNC XNI XNM XNS RHX RLA which are no longer used in Oracle E-Business Suite Release 12, but may have been carried forward during database upgrades.

C

Processes Used by Oracle E-Business Suite

This appendix covers the following topics:

- Table of Processes Used by Oracle E-Business Suite

Table of Processes Used by Oracle E-Business Suite

Process Name	Description	Script
tnslsnr	Applications RPC listener process	`adalnctl.sh`
opmn	Process manager (starts httpd)	`adopmnctl.sh`
httpd	Apache Web Server Listener	`adapcctl.sh`
java -Dweblogic. Name=AdminServer	WebLogic Administration Server	`adadminsrvctl.sh`
java weblogic.NodeManager	Node manager	`adnodemgrctl.sh`
java -Dweblogic. Name=oacore_server1	oacore managed server	`admanagedsrvctl.sh start oacore_server1`
java -Dweblogic. Name=forms_server1	Forms managed server	`admanagedsrvctl.sh start forms_server1`
java -Dweblogic. Name=oafm_server1	oafm managed server	`admanagedsrvctl.sh start oafm_serverS1`

Process Name	Description	Script
FNDSM	Concurrent Manager	`adcmctl.sh`
FFTM		
RCVOLTM		
POXCON		
INTCM		
FNDCRM		
PALIBR		
MRCLIB		
FNDLIBR		
INVLIBR		
java oracle.apps.jtf.fm.engine.processor.Processor java oracle.apps.jtf.fm.engine.remote.RemoteCommand	Fulfillment Server process	`jtffmctl.sh`
	Forms Server (a)	`adformsrvctl.sh`

(a) The forms server (socket mode) is not recommended. The default in Oracle E-Business Suite Release 12 is servlet mode.

D

Ports Used by Oracle E-Business Suite

This appendix covers the following topics:

- Table of Ports Used by Oracle E-Business Suite
- Table of Ports Used by WebLogic Server

Table of Ports Used by Oracle E-Business Suite

Variable Name	Description	Default Value	Technology	Component
s_dbport	Port on the database server used by the database listener	1521	RDBMS	TNS listener
s_rpcport	RPC port on the concurrent processing server that receives incoming Report Review Agent requests	1626	Applications	Application tier TNS listener
s_formsport(a)	Port on the Forms server used by the Forms Listener	9000	Forms 10	Forms
s_mwaPortNo	MSCA Server Port Number	10200	Applications	Mobile

Variable Name	Description	Default Value	Technology	Component
s_mwaDispatcherPort	MSCA Dispatcher Port Number	10300	Applications	Mobile
s_webport	Port on the webserver where http server listens for non-TLS requests	8000	Oracle Fusion Middleware	Oracle HTTP Server
s_webssl_port	Port on the webserver where http server listens for TLS requests	4443	Oracle Fusion Middleware	Oracle HTTP Server
s_active_webport	Value of this variable is set to value of s_webport when Listener is configured in non-TLS mode and to the value of s_webssl_port when TLS is configured	8000/4443	Oracle Fusion Middleware	Oracle HTTP Server
s_jtfuf_port	JTF fulfilment server port	11000	Applications	JTF
s_ons_localport	Oracle Notification Service	6100	Oracle Fusion Middleware	OPMN (manages OHS & oc4j)
s_ons_remoteport	Oracle Notification Service	6200	Oracle Fusion Middleware	OPMN
s_ons_requestport	Oracle Notification Service	6500	Oracle Fusion Middleware	OPMN

Variable Name	Description	Default Value	Technology	Component
s_ohs_adminport	OHS Administration Proxy Port	9999		Oracle HTTP Server
s_java_object_cache_port	Java Object Cache Port	12345	Oracle Fusion Middleware	Java Object Cache

(a) Forms server (socket mode) is optional (and not recommended) in Oracle E-Business Suite Release 12. The default is servlet mode.

Table of Ports Used by WebLogic Server

Oracle E-Business Suite Release 12.2 uses WebLogic Server (WLS) as its servlet container. WLS uses the following ports:

Variable Name	Description	Default Value	Firewall Configuration	Technology	Component
s_nm_port	WLS Node Manager Port	5556		Oracle Fusion Middleware	WLS
s_wls_adminport	WLS Admin Server Port	7001	Internal application tiers assumed to be on same subnet	Oracle Fusion Middleware	WLS
s_wls_oacoreport	WLS OACORE Application Port	7201		Oracle Fusion Middleware	WLS
s_wls_formsport	WLS FORMS Application Port	7401		Oracle Fusion Middleware	WLS
s_wls_oafmport	WLS OAFM Application Port	7601		Oracle Fusion Middleware	WLS

Variable Name	Description	Default Value	Firewall Configuration	Technology	Component
s_wls_forms-c4wsport	WLS FORMS-C4WS Application Port	7801		Oracle Fusion Middleware	WLS
s_wls_wcportletport	WLS Portlet Application Port	8889		Oracle Fusion Middleware	WLS
s_wls_oaeaport	WLS OAEA Application Port	6801		Oracle Fusion Middleware	WLS

E

Security Checklist

This appendix covers the following topics:

- About the Security Checklist
- Overview
- Oracle TNS Listener Security
- Oracle Database Security
- Oracle Application Tier Security
- Oracle E-Business Suite Security
- Desktop Security
- Operating Environment Security

About the Security Checklist

This section contains a summary of this document's best practice suggestions and their page locations. Use this summary as a security reference guide or checklist.

Overview

- Keep software up-to-date
- Restrict network access to critical services
- Follow the principle of least privilege
- Monitor system activity
- Keep up-to-date on the latest security information
- Updated Technology Stack

Oracle TNS Listener Security

- Harden operating environment
- Add IP restrictions or enable Valid Node Checking
- Specify connection timeout
- Specify Class of Secure Transport for dynamic registration
- Enable encryption of network traffic
- Enable TNS listener password (only if required)
- Enable admin restrictions
- Enable TNS listener logging

Oracle Database Security

- Harden operating environment
- Disable XDB
- Review database links
- Remove operating system trusted remote logon
- Change default installation passwords
- Implement two profiles for password management
- Restrict access to SQL trace files
- Remove operating system trusted remote roles
- Limit file system access within PL/SQL
- Limit dictionary access
- Revoke unnecessary grants given to APPLSYSPUB
- Configure the database for auditing
- Audit database connections

- Audit database schema changes
- Audit other activities
- Audit administrators and their actions
- Review audit records
- Maintain audit records
- Secure audit records

Oracle Application Tier Security

- Harden operating environment
- Configure Allowed Resources
- Configure Allowed Redirects
- Protect administrative pages
- Configure logging

Oracle E-Business Suite Security

- Harden operating environment
- Set Workflow notification mailer SEND_ACCESS_KEY to N
- Ensure you know who is a Workflow admin
- Set tools environment variables
- Restrict file types that may be uploaded
- Enable Antisamy HTML filter
- Use certified HTTP security headers
- Use TLS to encrypt Oracle E-Business Suite connections
- Avoid weak ciphers and protocols for SSL (HTTPS)
- Use external web tier if exposing any part of Oracle E-Business Suite to the internet

- Use terminal services for client-server programs
- Change passwords for seeded application user accounts
- Switch to hashed passwords
- Tighten logon and session profile options
- Create new user accounts safely
- Create shared responsibilities instead of shared accounts
- Configure concurrent manager for safe authentication
- Configure concurrent manager for start and stop without the APPS password
- Activate server security
- Create DBC files securely
- Consider using single sign-on
- Review and limit responsibilities and permissions
- Set other security-related profile options
- Restrict responsibilities by web server trust level
- Set sign-on audit level
- Monitor system activity with OAM
- Retrieve audit records using Reports
- Retrieve audit records using SQL
- Purge audit records
- Review data tracked (no Reports available)
- Configuring Audit Trail
- Generate and identify audit trail objects
- Choose tables to audit
- Retrieve audit records using SQL

- Purge audit records
- References on Oracle E-Business Suite auditing

Desktop Security

- Configure browser
- Update browser
- Turn off AutoComplete
- Set policy for unattended PC sessions

Operating Environment Security

- Cleanup file ownership and access
- Cleanup file permissions
- Lockdown operating system libraries and programs
- Filter IP packets
- Prevent spoofing
- Eliminate Telnet, rsh, and FTP daemons
- Verify network configurations
- Monitor for attacks
- Configure accounts securely
- Limit root access
- Manage user accounts
- Secure NFS
- Secure operating system devices
- Secure executables
- Secure file access

F

Sign-On Audit Concurrent Manager Reports

This appendix covers the following topics:

- About Sign-On Audit Concurrent Manager Reports
- Sign-On Audit Concurrent Requests Report
- Sign-On Audit Forms Report
- Sign-On Audit Responsibilities Report
- Sign-On Audit Unsuccessful Logins Report
- Sign-On Audit Users Report

About Sign-On Audit Concurrent Manager Reports

The following information details the various Sign-On Audit Concurrent Manager reports. This appendix assumes that you have read and implemented the configuration as defined in Sign-On Audit, page 16-3.

Sign-On Audit Concurrent Requests Report

Use this report to view information about who is requesting what concurrent requests and from which responsibilities and forms.

> **Important:** You can only generate Sign-On Audit Concurrent Requests Reports for those users you are auditing.

The following table describes the parameters included in each report:

Sign-On Audit Concurrent Requests Report Parameters

Report Parameter	Description
Sort By	Sort the information in your report by operating system login name, the requested start date, and/or application user name.
Login Name	Search for a specific login name that meets your other search criteria. If you leave this parameter blank, your report contains all login names that meet your other search criteria.
User Name	Search for a specific application user name that meets your other search criteria. If you leave this parameter blank, your report contains all application user names that meet your other search criteria.
From Request Start Time/To Request Start Time	Search for concurrent requests that meet your other search criteria and have requested start times in a specific time period. Use these parameters to specify the start and end of your time period. If you leave these parameters blank, your report contains concurrent requests from any date that also meet your other search criteria to the current date for this parameter.

The parameter values entered in the search criteria is included in the report heading.

Report results are organized in columns which are described in the following table:

Sign-On Audit Concurrent Requests Report Column Headings

Column Heading	Description
Login Name	The operating system login name of the user who submitted the concurrent request.

Column Heading	Description
Request ID	The concurrent request ID of the submitted concurrent request. Use the Concurrent Requests form to view completion information for a concurrent request ID.
Concurrent Program Name	The name of the concurrent program the user submitted. Use the Concurrent Programs form to view detail information about a concurrent program.
User Name	The Oracle E-Business Suite user name of the user who submitted the concurrent request. Use the Users form to view detail information about an application user. See: Users Window, page 4-26.
Responsibility Name	The name of the responsibility from which the user submitted the concurrent request. The responsibility displays only if you audited the user at the responsibility or form Sign-on Audit level. Use the Responsibilities form to view detailed information about a responsibility. See: Responsibilities Window, page 4-22.
Form Name	The name of the form from which the user submitted the concurrent request. The form name displays only if you audited the user at the form Sign-On Audit level.
Requested Start Time	The date and time the concurrent request started running.

Sign-On Audit Forms Report

Use this report to view who is navigating to what form and when they do it.

> **Note:** You can only generate a Sign-On Audit Forms Report for those users you are auditing.

The following table describes the parameters included in each report:

Sign-On Audit Forms Report Parameters

Report Parameter	Description
Sort By	Sort the information in your report by the time users entered or left a form, the name of the form that users access, the operating system login name of the user, the responsibility users access, the terminal that users are on, and/or the application user name.
Login Name	Search for information about a specific login name that meets your other search criteria. If you leave this parameter blank, your report contains all login names that meet your other search criteria.
User Name	Search for information about a specific application user name that meets your other search criteria. If you leave this parameter blank, your report contains all application user names that meet your other search criteria.
Terminal Name	Search for information about a specific terminal that meets your other search criteria. If you leave this parameter blank, your report contains all terminal names that meet your other search criteria.
Responsibility Name	Search for information about a specific responsibility that meets your other search criteria. If you leave this parameter blank, your report contains all responsibilities that meet your other search criteria.
Form Name	Search for information about a specific form that meets your other search criteria. If you leave this parameter blank, your report contains all forms that also meet your other search criteria.

Report Parameter	Description
From Active Date/To Active Date	Search for information about forms accessed by users within a specific time period and that meet your other search criteria. Use these parameters to specify the start and end of your time period. If you leave these parameters blank, your report contains forms accessed from any date that also meet your other search criteria to the current date for this parameter.

The parameter values entered in the search criteria is included in the report heading.

Report results are organized in columns which are described in the following table:

Sign-On Audit Forms Report Column Headings

Column Heading	Description
User Name	The Oracle E-Business Suite user name of the user who last accessed the responsibility. Use the Users form to view detailed information about an application user. See: Users Window, page 4-26.
Login Name	The operating system login name of the user who accessed the form.
Terminal Name	The operating system ID of the terminal from which the user accessed the form.
Responsibility Name	The name of the responsibility from which the user accessed the form. The responsibility displays only if you audited the user at the responsibility or form Sign-on Audit level. Use the Responsibilities form to view detailed information about a responsibility. See: Responsibilities Window, page 4-22.
Start Active Time/End Active Time	The dates and times when the user accessed/exited the form. The start active time and end active time display only if you audited the user at the form Sign-on Audit level.

Column Heading	Description
Form Name	The name of the form that the user accessed. The form name displays only if you audited the user at the form Sign-on Audit level.
Last Active Time	The last time the form was accessed.

Sign-On Audit Responsibilities Report

Use this report to view who is selecting what responsibility and when they do it.

> **Important:** You can only generate Sign-On Audit Responsibilities Reports for those users you are auditing.

The following table describes the parameters included in each report:

Sign-On Audit Responsibilities Report Parameters

Report Parameter	Description
Sort By	Sort the information in your report by the time users entered or left a responsibility, the operating system login name of the user, the responsibility name, the terminal that users are on, and/or the application user name.
Login Name	Search for information about a specific login name that meets your other search criteria. If you leave this parameter blank, your report contains all login names that meet your other search criteria.
User Name	Search for information about a specific application user name that meets your other search criteria. If you leave this parameter blank, your report contains all application user names that meet your other search criteria.

Report Parameter	Description
Terminal Name	Search for information about a specific terminal that meets your other search criteria. If you leave this parameter blank, your report contains all terminal names that meet your other search criteria.
Responsibility Name	Search for information about a specific responsibility that meets your other search criteria. If you leave this parameter blank, your report contains all responsibilities that meet your other search criteria.
From Active Date/To Active Date	Search for information about responsibilities accessed by users within a specific time period and that meet your other search criteria. Use these parameters to specify the start and end of your time period. If you leave these parameters blank, your report contains responsibilities accessed from any date that also meet your other search criteria to the current date for this parameter.

The parameter values entered in the search criteria is included in the report heading.

Report results are organized in columns which are described in the following table:

Sign-On Audit Responsibilities Report Column Headings

Column Heading	Description
User Name	The Oracle E-Business Suite user name of the user who last accessed the responsibility. Use the Users form to view detail information about an application user. See: Users Window, page 4-26.
Login Name	The operating system login name of the user who selected the responsibility.
Terminal Name	The operating system ID of the terminal from which the user selected the responsibility.

Column Heading	Description
Responsibility Name	The name of the responsibility the user used. The responsibility displays only if you audited the user at the responsibility or form Sign-on Audit level. Use the Responsibilities form to view detailed information about a responsibility. See: Responsibilities Window, page 4-22.
Start Active Time/End Active Time	The dates and times when the user selected/exited the responsibility. The start active time and end active time display only if you audited the user at the responsibility or form Sign-On Audit level.
Last Active Time (starting with Release 12.2.10 and later or R12. ATG_PF.C.Delta.9)	The last active time when the responsibility was accessed.

Sign-On Audit Unsuccessful Logins Report

Use this report to view who unsuccessfully attempted to sign on to Oracle E-Business Suite as another user. An unsuccessful login occurs when a user enters either an incorrect user name or an incorrect password. The report will only display user names that exist in the Oracle E-Business Suite database. If an attempt is made to log in with user name that does not exist, it will be reported on this report as "ANONYMOUS." You can generate Sign-On Audit Unsuccessful Logins Reports for any users, regardless of whom you are auditing.

The following table describes the parameters included in each report:

Sign-On Audit Unsuccessful Logins Report Parameters

Report Parameter	Description
Sort By	Sort the information in your report by the time users attempt to login, operating system login name of the user, the terminal that users are on, and/or the application user name.

Report Parameter	Description
Login Name	Search for information about a specific login name that meets your other search criteria. If you leave this parameter blank, your report contains all login names that meet your other search criteria.
User Name	Search for information about a specific application user name that meets your other search criteria. If you leave this parameter blank, your report contains all application user names that meet your other search criteria.
Terminal Name	Search for information about a specific terminal that meets your other search criteria to make your report as brief as you need. If you leave this parameter blank, your report contains all terminal names that meet your other search criteria.
From Attempt Date/To Attempt Date	Search for information about unsuccessful logins within a specific time period and that meet your other search criteria. Use these parameters to specify the start and end of your time period. If you leave these parameters blank, your report contains unsuccessful logins from any date that also meet your other search criteria to the current date for this parameter.

The parameter values entered in the search criteria is included in the report heading.

Report results are organized in columns which are described in the following table:

Sign-On Audit Unsuccessful Logins Report Column Headings

Column Heading	Description
User Name	The Oracle E-Business Suite user name of the user who unsuccessfully tried to sign on. Use the Users form to view detail information about an application user.

Column Heading	Description
Login Name	The operating system login name of the user who unsuccessfully tried to sign on.
Terminal	The operating system ID of the terminal from which the user unsuccessfully tried to sign on.
Attempt Time	The date and time when the user unsuccessfully tried to sign on. See: Monitor Users, page 16-6.

Sign-On Audit Users Report

Use this report to view who signs on and for how long.

> **Important:** You can only generate Sign-On Audit Users Reports or those users you are auditing.

The following table describes the parameters included in each report:

Sign-On Audit Users Report Parameters

Report Parameter	Description
Sort By	Sort the information in your report by the time users start or finish using an application user name, the operating system login name of the user, the terminal that users are on, and/or the application user name.
Login Name	Search for information about a specific login name that meets your other search criteria to make your report as brief as you need. If you leave this parameter blank, your report contains all login names that meet your other search criteria.

Report Parameter	Description
User Name	Search for information about a specific application user name that meets your other search criteria to make your report as brief as you need. If you leave this parameter blank, your report contains all application user names that meet your other search criteria.
Terminal Name	Search for information about a specific terminal that meets your other search criteria to make your report as brief as you need. If you leave this parameter blank, your report contains all terminal names that meet your other search criteria.
From Active Date/To Active Date	You can search for information about users logged into Oracle E-Business Suite within a specific time period and that meet your other search criteria. Use these parameters to specify the start and end of your time period. If you leave these parameters blank, your report contains user information from the first date that also meets your other search criteria to the current date.

The parameter values entered in the search criteria is included in the report heading.

Report results are organized in columns which are described in the following table:

Sign-On Audit Users Report Column Headings

Column Heading	Description
Session Number	The Oracle E-Business Suite session number that uniquely identifies each application user sign-on.
User Name	The Oracle E-Business Suite user name of the user who signed on. Use the Users form to view detailed information about an application user. See: Users Window, page 4-26.

Column Heading	Description
Login Name	The operating system login name of the user who signed on.
Terminal Name	The operating system ID of the terminal from which the user signed on.
Start Active Time/End Active Time	The dates and times when the user signed on and off from Oracle E-Business Suite. The start active time and end active time display only if you audited the user at the user Sign-On Audit level.
Oracle Process	The Oracle database process ID used during the user's sign-on. Consult your database administrator for more information concerning Oracle processes.
System Process	The operating system process ID used during the user's sign-on. Consult your operating system administrator for more information concerning your operating system process ID.
Client IP Address	The IP address of the client machine. This may be the IP address of a load balancer or reverse proxy if the configuration of those devices do not pass the client IP address through.

G

Additional References

References

The table below contains additional resource material useful for securing Oracle E-Business Suite.

My Oracle Support References

My Oracle Support Knowledge Document Number	Document Title
1375670.1	*Oracle E-Business Suite Release 12.2 Configuration in a DMZ*
1367293.1	*Enabling TLS in Oracle E-Business Suite Release 12.2*
1585296.1	*Using TDE Tablespace Encryption with Oracle E-Business Suite Release 12.2*
950018.1	*Enhancing Oracle E-Business Suite Security with Separation of Duties*
1306938.1	*FNDCPASS Troubleshooting Guide For Login and Changing Applications Passwords*
1334930.1	*Sensitive Objects and Administrative Pages in Oracle E-Business Suite*

My Oracle Support Knowledge Document Number	Document Title
1357849.1	*Security Configuration Mechanism in the Attachments Feature in Oracle E-Business Suite*
1573912.1	*All About Oracle Payments Release 12 Wallets And Payments Data Encryption*

H

Security Features for Earlier Oracle E-Business Suite Releases

Overview

This appendix provides reference to security features found in previous Oracle E-Business Suite releases.

FND: Security Resource Logging Profile Option Values for Earlier Releases

In Oracle E-Business Suite Release 12.2.6 with Patch 4737426:R12.FND.C through Release 12.2.10, the profile option FND: Security Resource Logging (FND_SEC_LOG_RESOURCES) can be set to one of the following values to log resource access:

- **ALL**: All requests of dispatcher type REQUEST, FORWARDS, INCLUDES are logged in simple format.
- **FORWARDS**: All requests of dispatcher type REJECTED and FORWARDS are logged in simple format.
- **FORWARDS, INCLUDES**: All requests of type FORWARDS and INCLUDES are logged in simple format. Rejected FORWARDS requests will also be logged. This is the default value.
- **NONE**: No requests are logged.
- **REJECTED**: All rejected requests of dispatcher type REQUEST and FORWARDS are logged in detailed format, regardless of the AFLOG_LEVEL profile value. Allowed requests are not logged.

- **REJECTED, FORWARDS, INCLUDES**: Only Rejected requests of dispatcher type FORWARDS are logged in detailed format irrespective of the AFLOG_LEVEL profile value.

  When the profile FND_SEC_LOG_RESOURCES is set to REJECTED or is set to REJECTED, FORWARDS, INCLUDES, then the logs will be in a detailed format. If the profile is set to any of the other values, then the logs will be in a simple format, unless AFLOG_LVEL profile is set to STATEMENT.

Obsolete Secure Configuration Console Checks

The following table lists profile options that were checked in prior versions of the Secure Configuration Console per the Checked Security Guidelines, page 13-3, but are now obsolete. These checks have been removed from the console or will be removed in a future release.

Obsolete Secure Configuration Console Checks for Security Guidelines

Profile Option Name	Code (Internal Name)
Audit Trail:Activate	AUDITTRAIL:ACTIVATE
Concurrent:Report Access Level	CONC_REPORT_ACCESS_LEVEL
Sign-On:Notification	SIGNONAUDIT:NOTIFY
IRC: XSS Filter	IRC_XSS_FILTER
FND: Security FileStreaming No-Store	FND_SEC_FILESTREAM_NO STORE

The following profile options were included in Oracle E-Business Suite Release 12 and have been end dated.

End-Dated Profile Options Previously Found in the Secure Configuration Console

Profile Option Name	Code (Internal Name)	Comments
FND Validation Level	FND_VALIDATION_LEVEL	FND Validation Level is defaulted to ERROR in Oracle E-Business Suite Release 12. This profile has been end dated and is not currently used.
Framework Validation Level	FRAMEWORK_VALIDATIO N_LEVEL	Framework Validation Level is defaulted to ERROR in Oracle E-Business Suite Release 12. This profile has been end dated and is not currently used.
FND Function Validation Level	FND_FUNCTION_VALIDAT ION_LEVEL	FND Function Validation Level is defaulted to ERROR in Oracle E-Business Suite Release 12. This profile has been end dated and is not currently used.

If any of the profile options listed in the tables of this section fail the Secure Configuration Console checks, you can either fix or suppress the failure. For a secure environment, Oracle recommends that you address all failures that are applicable to your environment.

Index

A

Access Control with Oracle User Management, 2-1
Account Creation by Administrators
  Access Control with Oracle User Management, 2-7
AFPASSWD utility
  using to change APPS database account password, 5-74
  using to reset user's password when switching back to local authentication, 5-48
  using to set local password, 5-27
  using when profile is updated to allow LOCAL access, 5-63
Allowed Redirects, 4-101
Allowed Resources
  Definition, 4-82
Allowlist, 4-82
Application users
  assigning one or more responsibilities, 4-1
  changing passwords, 4-26
  defining, 3-38, 4-26
  disabling application password, 4-26
  reporting on active users, 4-65
  start dates, 3-39
  user name characteristics, 4-26
AppsUserExport
  user migration utility, 5-78
Audit Groups Window, 18-25
Auditing user activity
  Sign-On Audit, 16-4
Audit Installations Window, 18-23
Audit Tables Window, 18-27
Audit Trail
  search pages, 18-30
authorization
  in single sign-on, 5-12

C

Case sensitivity
  in user passwords, 4-2
Collisions
  in bulk load, 5-84
configurable user name policy, 3-25
Connectors
  Oracle Identity Manager component, 5-3
cookie
  definition, 4-79
criterion
  in role administration, 3-32

D

Data Security, 4-18
  Access Control with Oracle User Management, 2-3
Data Security Policies
  Defining Data Security Policies, 3-14
Delegated Administration
  Access Control in Oracle E-Business Suite, 2-6
  Defining Delegated Administration Privileges for Roles
    Organization Administration, 3-9
    Role Administration, 3-9

User Administration, 3-9
disable inactive sessions
session timeout, 16-7

E

end-dating
roles, 3-31
Enterprise Command Center security, 4-2

F

FGA for RBAC, 3-31
Fine Grained Access for RBAC, 3-31
FND_SSO_UTIL APIs, 5-96
FNDCPASS utility, 4-3
using to change APPS database account password, 5-74
using to migrate passwords to non-reversible hash, 4-3
using to reset user's password when switching back to local authentication, 5-48
using to set local password, 5-27
using when profile is updated to allow LOCAL access, 5-63
Form Functions Window, 4-31
Forms
Define Menu, 4-31, 4-36
Monitor Application Users, 18-21
Responsibility, 4-22
Function Security
Access Control with Oracle User Management, 2-2
implementation, 4-16
Function Security Function Report, 4-62
Function Security Menu Report, 4-63
Function Security Menu Viewer
Menu Viewer, 4-39
Function Security Navigator Report, 4-63

G

GUEST User
password restriction, 4-2
Guest user account, 4-5
GUID, 5-11

H

HRMS Security, 4-2

I

ICX_SESSION_COOKIE_DOMAIN
Oracle Applications Session Cookie Domain Profile, 4-80

L

LDAPUserImport
user migration utility, 5-78
limited administrator
in FGA for RBAC, 3-32
Login Assistance, 3-55

M

Menus
compiling, 4-17, 4-62
defining, 4-36
defining a menu entry, 4-36
entering arguments, 4-33
menu prompts, 4-36
Menu Viewer, 4-39
role in function security, 4-1
sequence numbers, 4-36
Menus Window, 4-36
Menu Viewer, 4-39
Monitor Users Window, 18-21

N

Non-reversible hash password scheme, 4-2

O

OAM WebGate agent
used in Oracle E-Business Suite integration, 5-4
Oracle Access Manager
OAM, 5-1, 5-2
Oracle Access Manager WebGate
definition, 5-5
Oracle Directory Services, 5-1, 5-2
Oracle E-Business Suite AccessGate, 5-2
Oracle E-Business Suite security
defining a responsibility, 4-22
ORACLE ID
assigning to responsibility, 4-24

Oracle Identity Management
integration with Oracle E-Business Suite, 5-3
Oracle Identity Manager
use with Oracle E-Business Suite, 5-3
Oracle Internet Directory
OID, 5-2
Oracle Unified Directory, 5-2
Oracle User Management Setup Tasks
Defining Role Categories, 3-1
Organization Administration Privileges
Access Control in Oracle E-Business Suite , 2-6
Organization Contacts
Registering External Organization Contacts, 3-37

P

Page Access Tracking
in Proxy User mode, 3-52
Password
Resetting User Passwords, 3-29
Passwords
case-sensitive, 4-2
People
Maintaining People and Users, 3-27
Permissions
Assigning Permissions to Roles, 3-3
provisioning integrated application
definition, 5-16
provisioning profiles
definition, 5-16
Proxy User
Description, 2-16
proxy user feature
definition, 2-16
proxy users, 3-41

R

Registration Processes
Access Control with Oracle User Management, 2-7
Creating and Updating Registration Processes, 3-22
Reports
Active Responsibilities, 4-64
Active Users, 4-65
Concurrent Requests, F-1
Forms, F-3
Reports and Sets by Responsibility, 4-66
Responsibilities, F-6
Security Reports, 3-56
Unsuccessful Logins, F-8
Users, F-10
Users of a Responsibility, 4-63
REpresentational State Transfer security services, 4-67
Requests for Additional Access, 3-54
Access Control with Oracle User Management, 2-7
Responsibilities, 4-1
Application name, 4-23
deactivating, 4-23
defining, 4-22
major components, 4-6
predefined, 4-6
reporting on active responsibilities, 4-64
reporting on reports and report sets, 4-66
reporting on users of, 4-63
Start date, 4-23
Responsibilities Window, 4-22
REST services, 4-67
Role Administration Privileges
Access Control in Oracle E-Business Suite, 2-6
Role Based Access Control (RBAC)
Access Control with Oracle User Management, 2-3
Role Categories
Access Control with Oracle User Management, 2-3
Defining Role Categories, 3-1
Role Inheritance Hierarchies
Access Control with Oracle User Management, 2-3
Defining Role Inheritance Hierarchies
Deployment Options, 3-15
Roles
Assigning Permissions to Roles, 3-3
Assigning Roles to and Revoking Roles From Users, 3-30
Creating and Updating Roles, 3-2
Defining Delegated Administration Privileges for Roles
Organization Administration, 3-9
Role Administration, 3-9

User Administration, 3-9

S

Secure Configuration Console, 13-1
Security Administrator
  Proxy User Management, 2-17
Security groups, 4-10
Security Groups
  defining (for HRMS only), 4-25
Security Groups Window, 4-25
Security in Enterprise Command Centers, 4-2
Security in HRMS, 4-2
seeded user name policies, 3-25
Self Service Account Requests
  Access Control with Oracle User Management, 2-7
Self-Service and Approvals
  Access Control in Oracle E-Business Suite, 2-15
Self-Service Registration, 3-54
Session time-out, 4-5
Sign-On Audit, 16-4
  monitoring users, 18-21
Single Sign-On, 5-1
  profile options, 5-52
  user experience, 5-18
single sign-out
  definition, 5-3

T

target systems, 5-3
txkEBSAuth.xml
  Oracle E-Business Suite AccessGate configuration script, 5-9

U

UMX_PROXY_RESP_DISABLE profile option, 3-42
UMX_SYS_ACCT
  data security object, 2-7, 3-7, 3-37
UMX: Disable Proxy Responsibilities profile option, 3-42
Upgrading
  preserving custom menus, 4-17
User Accounts
  Creating, Inactivating, and Reactivating User Accounts, 3-29
User Administration Privileges
  Access Control in Oracle E-Business Suite, 2-6
Users, 4-1
  Assigning Roles to and Revoking Roles From Users, 3-30
  case-sensitive passwords, 4-2
  Maintaining People and Users, 3-27
  Resetting User Passwords, 3-29
User session limits, 4-5
Users Window, 4-26