Oracle® Fusion Applications Security Guide

11*g* Release 7 (11.1.7)

Part Number E16689-07

March 2013

Oracle® Fusion Applications Security Guide

Part Number E16689-07

Author: Tina Brand

Contributor: Mahesh Sabapathy

Contents

6 Data Security

7 Privacy

8 Enforcement Across Tools, Technologies, Data Transformations, and Access Methods

9 Segregation of Duties

10 Identity Management and Access Provisioning

11 Security Reference Implementation

12 Enforcement Across the Information Life Cycle

Preface

This Preface introduces the guides, online help, and other information sources available to help you more effectively use Oracle Fusion Applications.

Oracle Fusion Applications Help

You can access Oracle Fusion Applications Help for the current page, section, activity, or task by clicking the help icon. The following figure depicts the help icon.

You can add custom help files to replace or supplement the provided content. Each release update includes new help content to ensure you have access to the latest information. Patching does not affect your custom help content.

Oracle Fusion Applications Guides

Oracle Fusion Applications guides are a structured collection of the help topics, examples, and FAQs from the help system packaged for easy download and offline reference, and sequenced to facilitate learning. You can access the guides from the **Guides** menu in the global area at the top of Oracle Fusion Applications Help pages.

Guides are designed for specific audiences:

- **User Guides** address the tasks in one or more business processes. They are intended for users who perform these tasks, and managers looking for an overview of the business processes. They are organized by the business process activities and tasks.
- **Implementation Guides** address the tasks required to set up an offering, or selected features of an offering. They are intended for implementors. They are organized to follow the task list sequence of the offerings, as displayed within the Setup and Maintenance work area provided by Oracle Fusion Functional Setup Manager.
- **Concept Guides** explain the key concepts and decisions for a specific area of functionality. They are intended for decision makers, such as chief financial officers, financial analysts, and implementation consultants. They are organized by the logical flow of features and functions.
- **Security Reference Manuals** describe the predefined data that is included in the security reference implementation for one offering. They are

intended for implementors, security administrators, and auditors. They are organized by role.

These guides cover specific business processes and offerings. Common areas are addressed in the guides listed in the following table.

Guide	Intended Audience	Purpose
Common User Guide	All users	Explains tasks performed by most users.
Common Implementation Guide	Implementors	Explains tasks within the Define Common Applications Configuration task list, which is included in all offerings.
Functional Setup Manager User Guide	Implementors	Explains how to use Oracle Fusion Functional Setup Manager to plan, manage, and track your implementation projects, migrate setup data, and validate implementations.
Technical Guides	System administrators, application developers, and technical members of implementation teams	Explain how to install, patch, administer, and customize Oracle Fusion Applications. **Note** Limited content applicable to Oracle Cloud implementations.

For guides that are not available from the Guides menu, go to Oracle Technology Network at http://www.oracle.com/technetwork/indexes/documentation.

Other Information Sources

My Oracle Support

Oracle customers 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.

Use the My Oracle Support Knowledge Browser to find documents for a product area. You can search for release-specific information, such as patches, alerts, white papers, and troubleshooting tips. Other services include health checks, guided lifecycle advice, and direct contact with industry experts through the My Oracle Support Community.

Oracle Enterprise Repository for Oracle Fusion Applications

Oracle Enterprise Repository for Oracle Fusion Applications provides details on service-oriented architecture assets to help you manage the lifecycle of your

software from planning through implementation, testing, production, and changes.

In Oracle Fusion Applications, you can use Oracle Enterprise Repository at http://fusionappsoer.oracle.com for:

- Technical information about integrating with other applications, including services, operations, composites, events, and integration tables. The classification scheme shows the scenarios in which you use the assets, and includes diagrams, schematics, and links to other technical documentation.
- Other technical information such as reusable components, policies, architecture diagrams, and topology diagrams.

Note
The content of Oracle Enterprise Repository reflects the latest release of Oracle Fusion Applications.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/us/corporate/accessibility/index.html.

Comments and Suggestions

Your comments are important to us. We encourage you to send us feedback about Oracle Fusion Applications Help and guides. Please send your suggestions to oracle_fusion_applications_help_ww_grp@oracle.com. You can use the **Send Feedback to Oracle** link in the footer of Oracle Fusion Applications Help.

1

Introduction

Security: Overview

Oracle Fusion Applications is secure as delivered.

The security approach consists of tightly coordinating the following aspects of security.

- Role-based access control (RBAC)
- Function security
- Data security
- Privacy
- Access provisioning and identity management
- Segregation of duties policies
- Enforcement across tools, technologies, data transformations, and access methods
- Enforcement across the information life cycle

The Oracle Fusion Applications security approach supports a reference implementation of roles and security policies that address common business needs. Enterprises address needs specific to their organization by changing or extending the role definitions, role hierarchies, data security, and segregation of duties policies of the reference implementation.

Role-Based Access Control

Access to system resources is granted to users through the roles assigned to them, not to the users directly. Roles provide access to functions and data.

The Oracle Fusion Applications security approach includes abstract, job, duty, and data roles. Abstract roles group users without respect to specific jobs, such as all employees or all managers. Job roles group users in adherence to the principle of least privilege by granting access only in support of the duties likely to be performed, such as the job of Accounts Payable Manager. Duty roles define the duties of a job as entitlement to perform a particular action, such as processing payables invoices. Data roles group users who have functional access through a particular job role with access to a particular dimension of

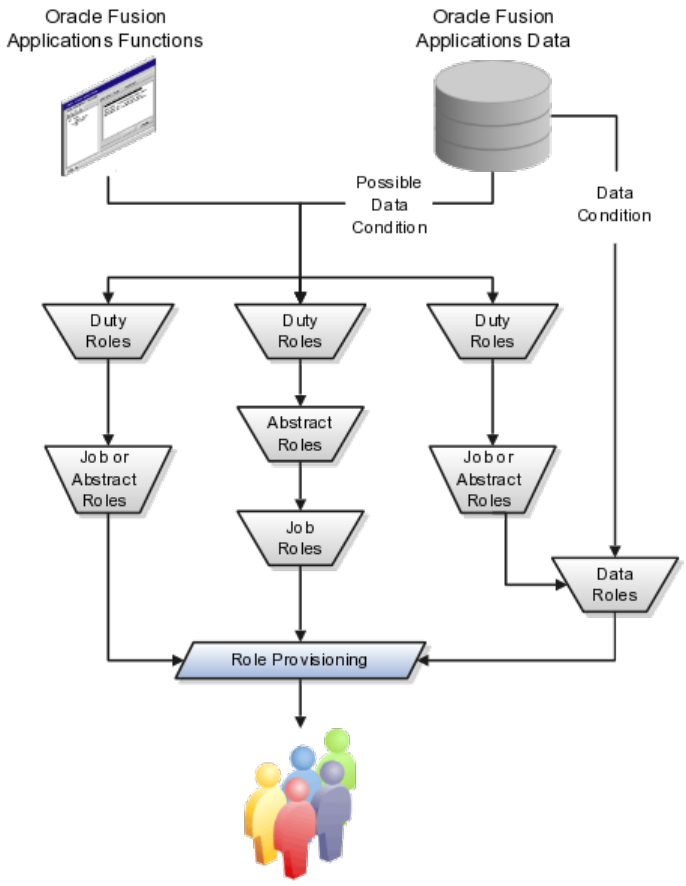
data, such as invoices relevant only to their business unit, or based on Human Capital Management (HCM) security profiles, such as employees who work in departments in a particular country, line of business, or division.

Abstract, job, and data roles are implemented as enterprise roles in Oracle Fusion Middleware so they can be shared across the enterprise. Duty roles are implemented as application roles in Oracle Fusion Middleware so they can be defined within applications.

Function and Data Security

Functions and data are inaccessible to users unless they are provisioned with the roles necessary to gain access. Function security provides users with access to pages in application users interfaces and actions that can be performed there. Data security allows users to see data in those pages. Some data is not secured, in which case access to a user interface page gives unrestricted access to the data that is accessible from that page. For example, some setup data such as Receivables Receipt Method and Payment Method is not secured, and some transaction data such as Receivables Customer Profile is not secured. Archive data such as Receivables Archive is also not secured.

Enterprise roles inherit application roles that provide the enterprise roles with access to application functions and data. Roles are grouped hierarchically to reflect lines of authority and responsibility. The figure shows user access to functions and data determined by roles arranged in hierarchies and provisioned to the user.



Duty roles carry entitlement to actions on functions and data. An example of a duty role is the Payables Invoice Processing Duty. Job and abstract roles inherit duty roles that determine the access to functions appropriate to the job. For example, the job role Accounts Payable Manager inherits the Payables Invoice Processing Duty.

Data security policies may grant actions on data to enterprise or duty roles. The condition of a data security policy determines if the access is explicit, such as all invoices of a particular business unit, or implicit, such as all invoices in the business unit to which a user is assigned. Job and abstract roles inheriting duty roles for which data security policies are defined grant implicit data access.

Data roles inherit abstract or job roles or both, and are granted explicit access to data. For example, a job role might give view access to the functions needed to access invoices, but a data role that inherits the job role gives view access to the invoices data within a business unit, such as the data role Accounts Payable Manager - US which inherits the job role Accounts Payable Manager for performing accounts payable duties against the US business unit.

Authorization Policy Manager (APM) is available in Oracle Fusion Applications through integration with Oracle Identity Management (OIM). Authorization policy management involves managing duty roles, data role templates, and data security policies, as well as previewing data roles generated based on data role templates.

Privacy

Privacy encompasses data that should not be available to other individuals and organizations. Where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use.

Oracle Fusion applications classify data at several levels of sensitivity, and define privacy attributes that participate in data security policies to apply appropriate protections to sensitive data. Oracle Fusion Applications secures the privacy attributes of personally identifiable information (PII) consistently across Oracle Fusion applications, and controls the destination of privacy attributes to the fewest and most highly secured locations possible, such as limiting the attributes that HCM applications share with the Lightweight Directory Access Protocol (LDAP) store.

Access Provisioning and Identity Management

The Oracle Fusion Applications installation process creates an initial user and provisions that user with the administration roles necessary for initial setup.

Oracle Identity Management (OIM) is available in Oracle Fusion Applications through integration with Oracle Fusion Middleware. Identity management in Oracle Fusion Applications involves creating and managing user identities, creating and linking user accounts, managing user access control through user role assignment, managing enterprise roles, and managing OIM workflow approvals and delegated administration.

Through OIM, Oracle Fusion Applications notifies the IT security manager of all of the user requests (user life cycle changes), role provisioning requests, and grants to ensure role administration is always documented, authorized, and auditable.

Provision data roles, when available, and not the job or abstract roles the data roles inherit. In the absence of data roles, provision the abstract or job roles directly.

Segregation of Duties

Segregation of duties (SOD) separates activities such as approving, recording, processing, and reconciling results so an enterprise can more easily prevent or detect unintentional errors and willful fraud.

SOD policies constrain duties across roles so unethical, illegal, or damaging activities are less likely. SOD policies express constraints between role pairs.

Oracle Fusion role definitions respect segregation of duties policies. Oracle Fusion Applications is certified to integrate with Application Access Controls Governor (AACG) in the Oracle Enterprise Governance, Risk and Compliance (GRC) suite to ensure effective SOD.

Enforcement Across Tools, Technologies, Data Transformations, Access Methods, and Information Life Cycle

The Oracle Fusion Applications security approach enforces security controls across tools, technology infrastructure, transformations of data, access methods and the information life cycle.

The infrastructures of an Oracle Fusion Applications deployment vary from one tool in the technology stack to another, however the security approach coordinates transactional and analytical security so that all security policies and controls prevail across access methods and data transformations of enterprise information. Oracle Fusion Applications enforce each single statement of security policy through the multiple transformations of data necessary for transactions, dimensional analysis, and search optimization.

Oracle Fusion Applications optionally respect the Information Life Cycle Management policies that your enterprise establishes. Transparent Data Encryption (TDE) and Oracle Database Vault (ODV) protect data in transit and at rest, across the phases of a deployment from installation and setup, to archive and purge, and across databases from development to production.

Reference Implementation

The security reference implementation consists of roles, policies, and templates for generating data roles.

The security reference implementation consists of the following.

- Set of abstract and job roles
- Duty roles and role hierarchy for each job role and abstract role
- Privileges required to perform each duty defined by a duty role
- Data security policies for each job role, abstract role, or data role
- Predefined HCM security profiles
- Policies that protect personally identifiable information
- Mapping of data security policies to fact and dimension to ensure enforcement across tools and access methods

- Segregation of duties policies respected in the design of duties for the job role
- Segregation of duties conflicts in some job role definitions
- Templates for generating data roles and data security policies defined for those data roles
- Template of data masking algorithm

An enterprise changes the reference implementation to accommodate its particular business needs, thereby creating the enterprise's security implementation, leaving the reference implementation in place as a baseline. Upgrades preserve enterprise changes.

The security reference implementation can be viewed in the user interfaces where security tasks are performed or in the security reference manual (SRM) for each Oracle Fusion Applications offering.

Oracle Fusion Applications Security Business Fit: Explained

Security must be implemented to fit the business.

Oracle Fusion Applications supports an extensive predefined business process model (BPM) that is secured by a reference implementation of predefined roles and security policies.

Security Reference Implementation

The security reference implementation associates a full range of predefined roles with the business process model (BPM) levels. When assigned to users, the enterprise roles guide and control access to the task flows of the BPM and associated data. At the task level, task flows define the business actions that fulfill the intent of the BPM.

A security reference manual (SRM) for each offering presents all predefined roles, role hierarchies, business objects the roles must access, segregation of duties policies, and jobs that may have conflicting duties according to those policies. The reference implementation also can be viewed using the integrated Authorization Policy Manager (APM) and Oracle Identity Management (OIM) user interface pages to manage security policies, users, and identities.

Security: Information Roadmap

This roadmap lists the wide range of available information resources that are about or relevant to understanding Oracle Fusion Applications security.

The information resources cover the following areas.

- Oracle Fusion Applications
- Oracle Fusion Middleware
- Application Access Control Governor in the Oracle Enterprise Governance, Risk and Compliance (GRC) suite
- Oracle Database

Caution

Refer specifically to the Oracle Fusion Applications Edition of the following guides included in this roadmap.

- Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management
- Oracle Fusion Middleware Administrator's Guide for Authorization Policy Manager

Oracle Fusion Applications

Oracle Fusion Applications installation, deployment, administration, development, and extensibility information supports optimizing the security approach in the application tier. In addition to the resources listed below, each predefined Oracle Fusion Applications offering provides a Security Reference Manual.

- For an overview of built-in security in the context of deployment, refer to the Oracle Fusion Applications Enterprise Deployment Guide for Customer Relationship Management.

  See: Built In Security

- For information on the integration with Oracle Identity Management, see the following guides.

  See: Oracle Fusion Applications Installation Guide

  See: Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management

  - For information on using integrated Oracle Identity Management products when performing Oracle Fusion Applications security setup and implementation tasks, see the Oracle Fusion Middleware section, below.

- For a detailed functional explanation of the Oracle Fusion Applications security approach, see the following guides. Oracle Fusion Applications Security Hardening Guide is not relevant for Oracle Cloud implementations.

  See: Oracle Fusion Applications Security Guide

  See: Oracle Fusion Applications Security Hardening Guide

- For information about the security reference implementation common to all implementations, including the role hierarchies and policies in effect for common roles such as Application Implementation Consultant, Application Administrator, and IT Security Manager, see the following guide.

  See: Oracle Fusion Applications Common Security Reference Manual

- For information on administrative tasks to secure Oracle Fusion Applications, refer to the Oracle Fusion Applications Administrator's Guide

See: Securing Oracle Fusion Applications

- For information on configuring audit policies and the audit store, refer to the Oracle Fusion Applications Administrator's Guide. Audit Trail is not relevant in Oracle Cloud implementations.

  See: Configuring Audit Trail

- For understanding security architecture supporting Oracle Fusion Applications, refer to the Oracle Fusion Applications Developer's Guide

  See: Getting Started with Security

  - For information on implementing and running diagnostics on data security for new applications functionality, refer to the Oracle Fusion Applications Developer's Guide.

    See: Implementing Oracle Fusion Data Security

- For information on securing new business objects in Customer Relationship Management (CRM) Application Composer, refer to the Oracle Fusion Applications Extensibility Guide.

  See: Customizing Security for Custom Business Objects

- For information on securing new business objects in an extended application, refer to the Oracle Fusion Applications Extensibility Guide.

  See: Customizing Security for ADF Application Artifacts

Oracle Fusion Middleware

Oracle Fusion Middleware provides a foundation of identity management, authorization policy management, and security infrastructure in the middle tier.

- Authorization Policy Manager (APM) is available in Oracle Fusion Applications through integration with Oracle Identity Management (OIM). Authorization policy management involves managing duty roles, data role templates, and data security policies.

  See: Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide

- Oracle Identity Management (OIM) is available in Oracle Fusion Applications through integration with Oracle Fusion Middleware. Identity management in Oracle Fusion Application involves creating and managing user identities, creating and linking user accounts, managing user access control through user role assignment, managing enterprise roles, and managing workflow approvals and delegated administration.

  See: Oracle Fusion Middleware User's Guide for Oracle Identity Manager

  - For information about configuring user attributes and password policies, refer to the Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager.

    See: Configuration

- The Oracle Fusion Applications security approach uses as a foundation Oracle Fusion Middleware security.

See: Oracle Fusion Middleware Security Overview

See: Oracle Fusion Middleware Application Security Guide

- For information about auditing the Oracle Platform Security Service (OPSS) in Authorization Policy Manager (APM), Oracle Internet Directory (OID), and Oracle Virtual Directory, refer to the Oracle Fusion Middleware Application Security Guide. Audit Trail is not relevant in Oracle Cloud implementations.

  See: Configuring and Managing Auditing

  See: What Components Can be Audited

  - Oracle Fusion Middleware Audit Framework provides a set of predefined reports for Oracle Fusion Middleware components.

    See: Using Audit Analysis and Reporting

Oracle Application Access Controls Governor

Application Access Controls Governor in the Oracle Enterprise Governance, Risk and Compliance (GRC) suite provides transaction, preventive, and configuration controls for segregation of duties (SOD).

- Oracle Fusion Applications is certified to integrate with Applications Access Controls Governor (AACG) in the Oracle Enterprise Governance, Risk and Compliance (GRC)) suite to ensure effective SOD.

  See: Oracle Application Access Controls Governor Users Guide

  See: Oracle Application Access Controls Governor Implementation Guide

Oracle Database

Oracle Database supports application data security in the data tier. The Oracle Fusion Applications security approach is certified to use a foundation of Oracle Database security features. Information about securing Oracle Database is not relevant for Oracle Cloud implementations. Information about securing Oracle Database is not relevant for Oracle Cloud implementations.

- For information on using Transparent Data Encryption (TDE) and other advanced database security features, refer to the following guides.

  See: Oracle Database Security Guide

  See: Oracle Database Advanced Security Administrator's Guide

  See: Oracle Database Vault Administrator's Guide

  - For more information about data masking, refer to Data Masking Best Practices, an Oracle White Paper on Oracle Technology Network (http://www.oracle.com/technetwork).
  - For information on column masking and using Oracle Virtual Private Database to control data access, refer to the following guide.

    See: Oracle Database Security Guide

- For information about using and connecting to a Lightweight Directory Access Protocol (LDAP) store, refer to the following guides

  See: Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory

  See: Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory

Differences in Security Terminology: Explained

In some cases, terminology used within and outside of Oracle Fusion Applications differs based on vantage point. For example, Oracle Fusion Middleware and Oracle Application Access Control Governor provide a foundation that is integrated with, but external to, the Oracle Fusion Application suite.

The table shows how Oracle Fusion Applications, Oracle Fusion Middleware, Oracle Application Access Control Governor, and some possibly coexistent applications refer to various equivalent elements of security.

Note

Oracle Authorization Policy Manager and Oracle Identity Management are in Oracle Fusion Middleware, and Oracle Application Access Controls Governor is in Oracle Enterprise Governance, Risk and Compliance (GRC).

The equivalencies are true in general and based on the functional meaning of the terms. In the table, an empty cell indicates that no equivalent term exists.

Oracle Fusion Applications Security Reference Manuals and other documentation	Authorization Policy Manager	Oracle Identity Management	Oracle Application Access Controls Governor	Applications coexistent with Oracle Fusion Applications
User	User	User		PeopleSoft user profile
External user, such as partner or supplier	User	External user		
Enterprise role	External role	Role		eBusiness Suite responsibility
Abstract role	External role	Role		PeopleSoft role
Data role	External role	Role		eBusiness Suite responsibility PeopleSoft data permission
Job role	External role	Role		eBusiness Suite top level menu PeopleSoft role

Duty role	Application role		Access control	eBusiness Suite submenu PeopleSoft role
Privilege	Entitlement or permission set		Access control	eBusiness Suite form function PeopleSoft data permission
Entitlement			GRC entitlement	
Segregation of duties policy			Access control	
Database resource	Database resource			Data object
Data security policy	Data security policy			Data security grant
Data security policy	Entitlement policy			
Function security policy	Resource policy			Privilege grant
Function security policy	Entitlement policy			
Condition				Instance set

FAQs for Security Introduction

What's the difference between function security and data security?

Function security is a statement of what actions you can perform in which user interface pages.

Data security is a statement of what action can be taken against which data.

Function security controls access to user interfaces and actions needed to perform the tasks of a job. For example, an accounts payable manager can view invoices. The Accounts Payable Manager role provisioned to the accounts payable manager authorizes access the functions required to view invoices. Function security is also sometimes called application security and controlled by duty roles.

Data security controls access to data. In this example, the accounts payable manager for the North American Commercial Operation can view invoices in the North American Business Unit. Since invoices are secured objects, and a data role template exists for limiting the Accounts Payable Manager role to the business unit for which the provisioned user is authorized, a data role inherits the job role to limit access to those invoices that are in the North American Business Unit. Objects not secured explicitly with a data role are secured implicitly by the data security policies of the job role.

Both function and data are secured through role-based access control.

2

Security Tasks

Security Tasks: Highlights

Security tasks include the following.

- Security setup
- Security implementation and administration

Note

Security setup and administration tasks typically use integrated user interface pages that are provided by the following products.

- Oracle Identity Manager (OIM)
- Oracle Authorization Policy Manager (APM)
- Oracle Fusion Human Capital Management (HCM) products
- Oracle Application Access Control Governor (AACG) in Oracle Enterprise Governance, Risk and Compliance (GRC)

Security setup and administrative tasks performed by product administrators and implementation consultants, such as managing HCM security profiles, are presented in the documentation for those products.

Set Up the IT Security Manager Job Role

Provision the IT Security Manager job role with roles for user and role management.

- Using the OIM Administrator user name and password, sign in to Oracle Identity Manager (OIM). Refer to the Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition).

  See: Creating Users and Groups

- Open the IT Security Manager job role's attributes and use the Hierarchy tab to add the User Identity Administrators role and the Role Administrators role in the OIM Roles category using the Add action. Use the Delegated Administration menu to search for the Xellerate Users organization and assign it to the IT Security Manager role. Refer to the Oracle Fusion Middleware User's Guide for Oracle Identity Manager.

See: User Management Tasks

Prerequisite Tasks for Security Administration

Sign into Oracle Fusion Applications for the first time with the Installation Super User account to synchronize LDAP users with HCM user management and create an IT security manager user account and provision it with the IT Security Manager role. For environments that are not in Oracle Cloud, use the super user account that was created during installation to sign in for the first time.

- Installation establishes the super user account. Refer to the Oracle Fusion Applications Installation Guide.

  See: Identity Management Configuration

- Oracle provides an initial user for accessing your services in Oracle Cloud. For more information, refer to "Oracle Cloud Application Services Security: Explained" in Oracle Cloud documentation.
- Synchronize LDAP users with HCM user management by performing the Run User and Roles Synchronization Process task. Monitor completion of the predefined Enterprise Scheduler process called Retrieve Latest LDAP Changes.
- Refer to information about creating person records in Oracle Fusion Applications Workforce Development Implementation Guide, or refer to the Oracle Fusion Middleware User's Guide for Oracle Identity Manager.

  See: Managing Users

  - As a security guideline, provision a dedicated security professional with the IT Security Manager role as soon as possible after initial security setup and revoke that role from users provisioned with the Application Implementation Consultant role. If entitled to do so, see Security Tasks and Oracle Fusion Applications: How They Fit Together for details about provisioning the IT security manager.

Required Security Administration Tasks

Establish at least one implementation user and provision that user with sufficient access to set up the enterprise for all integrated Oracle Fusion Middleware and all application pillars or partitions.

- Perform the initial security tasks. If entitled to do so, see Initial Security Administration: Critical Choices.
  - Sign in to Oracle Fusion Applications using the IT security manager's or administrator's user name and password, and create and provision users who manage your implementation projects and set up enterprise structures by performing the Create Implementation Users task. Refer to the Oracle Fusion Middleware User's Guide for Oracle Identity Manager.

    See: User Management Tasks

  - Create a data role for implementation users who will set up HCM that grants access to data in secured objects required for performing HCM setup steps. Provision the implementation user with this View All data role. See "Creating an HCM Data Role: Worked Example."

- For an overview of security tasks from the perspective of an applications administrator, refer to the Oracle Fusion Applications Administrator's Guide

  See: Securing Oracle Fusion Applications

Optional Security Administration Tasks

Once initial security administration is complete and your enterprise is set up with structures such as business units, additional security administration tasks are optional and based on modifying and expanding the predefined security reference implementation to fit your enterprise. See points to consider for defining security, data security and trading partner security after enterprise setup.

- Create users. Refer to the Oracle Fusion Middleware User's Guide for Oracle Identity Manager.

  See: Creating Users

- Provision users with roles. Refer to the Oracle Fusion Middleware User's Guide for Oracle Identity Manager.

  See: Adding and Removing Roles

  - You manage users and job roles, including data and abstract roles, in Oracle Identity Management user interface pages. Refer to the Oracle Fusion Middleware User's Guide for Oracle Identity Manager.

    See: User Interfaces

  - You manage duties, security policies, and data role templates in the Authorization Policy Manager. Refer to the Oracle Fusion Middleware Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition).

    See: Managing Oracle Fusion Applications Data Security Policies

  - You manage role provisioning rules in Human Capital Management (HCM). Refer to the Role Mappings: Explained topic in the Oracle Fusion Applications Workforce Development Implementation Guide.

    See: Common Applications Configuration: Define Security for Human Capital Management

- For a complete description of the Oracle Fusion Applications security reference implementation, see the Oracle Fusion Applications Security Reference Manuals for each offering.

  See: Oracle Fusion Applications Common Security Reference Manual

- For a detailed functional explanation of the Oracle Fusion Applications security approach, refer to the following guides.

  See: Oracle Fusion Applications Security Guide

  See: Oracle Fusion Applications Security Hardening Guide

  - Since security in Oracle Fusion Applications is based on integrations with Oracle Identity Management in Fusion Middleware, security features in the database, and Oracle Enterprise Governance, Risk and

Compliance (GRC), additional resources in support of performing security tasks include the following.

- Authorization Policy Manager (APM) is available in Oracle Fusion Applications through integration with Oracle Identity Management (OIM). Authorization policy management involves managing duty roles, data role templates, and data security policies. Refer to the Oracle Fusion Middleware Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition).

  See: Getting Started With Oracle Authorization Policy Manager

- Oracle Identity Management (OIM) is available in Oracle Fusion Applications through integration with Oracle Fusion Middleware. Identity management in Oracle Fusion Application involves creating and managing user identities, creating and linking user accounts, managing user access control through user role assignment, managing enterprise roles, and managing workflow approvals and delegated administration.

  See: Oracle Fusion Middleware User's Guide for Oracle Identity Manager

- Oracle Fusion Applications is certified to integrate with Applications Access Controls Governor (AACG) in the Oracle Enterprise Governance, Risk and Compliance (GRC) suite to ensure effective segregation of duties (SOD).

  See: Oracle Application Access Controls Governor Users Guide

  See: Oracle Application Access Controls Governor Implementation Guide

- Configure and manage auditing. Refer to the Oracle Fusion Middleware Application Security Guide.

  See: Configuring and Managing Auditing

Security Tasks and Oracle Fusion Applications: How They Fit Together

The major security tasks and their order within the context of an overall Oracle Fusion Applications implementation extend from security setup through production deployment audits.

The Oracle Fusion business process model (BPM) provides a sequence of security implementation tasks that includes the following.

- Security setup (Define Common Applications Configuration activity)
  - Define Implementation Users task group (optional)
    - Create Implementation Users task
    - Create Data Role for Implementation Users task
    - Provision Roles to Implementation Users task

- Define security - tasks vary depending on deployed Oracle Fusion product family
  - Revoke Data Role from Implementation Users task
  - Import Worker Users task
  - Import Partner Users task
  - Manage Duties task
  - Manage Job Roles task
  - Manage Application Access Controls task
- Define Automated Governance, Risk, and Performance Controls activity
  - Manage Application Access Controls task (AACG settings)
  - Manage Application Preventive Controls task
  - Manage Application Transaction Controls task
  - Manage Application Configuration Controls task

- User and role provisioning tasks
  - Implement Role Request and Provisioning Controls activity
    - Import Worker Users task
    - Import Partner Users task
    - Self Request User Roles task
    - Approve User and Role Provisioning Requests task
    - Assign User Roles task
    - Manage Supplier User Roles and User Role Usages task
    - Map and Synchronize User Account Details task
    - Tasks for viewing account details for self or others
    - Tasks for applying and managing various role provisioning rules
    - Tasks for running synchronization processes
- Security implementation and ongoing maintenance after setup (Manage IT Security activity)
  - Implement Function Security Controls
    - Create Job Role task
    - Import Worker Users task

        - Import Partner Users task
        - Manage Duties task
        - Manage Job Roles task
        - Manage Users task
      - Implement Data Security Controls
        - Manage Data Security Policies task
        - Manage Role Templates task
        - Manage Encryption Keys task
        - Manage Segment Security task
        - Manage Data Access Sets task
        - Define Security Profiles task group
  - Auditing tasks
    - Manage Security Audit, Compliance and Reporting activity
      - Manage Application Access Controls task

Note

Go live deployment does not require lockdown or specific security tasks because security is enforced across the test to production information life cycle.

Required Roles

The following enterprise roles are provisioned to a single super user that is set up by the Oracle Fusion Applications installation process, and to the initial user set up by Oracle for Oracle Cloud Application Services:

- Application Implementation Consultant
- IT Security Manager
- Application Administrators for the provisioned products

Initial security administration also includes provisioning the IT Security Manager role with Oracle Identity Management (OIM) roles for user and role management.

- Identity User Administrator
- Role Administrator

Additionally, the Xellerate Users organization must be assigned to the IT Security Manager role.

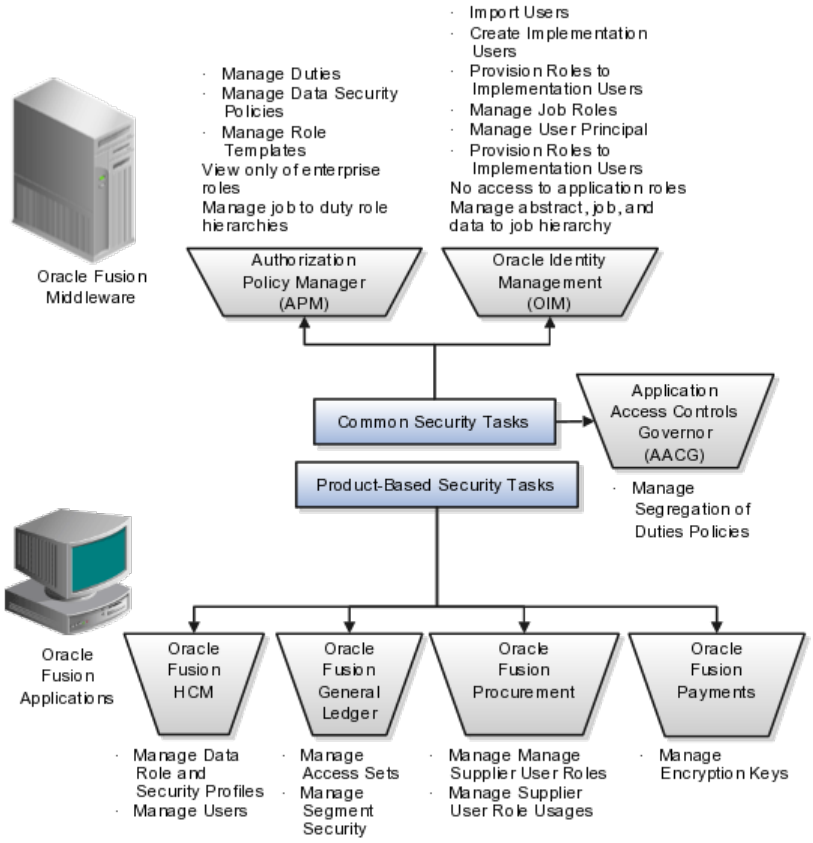
Important

As a security guideline, provision a dedicated security professional with the IT Security Manager role at the beginning of an implementation, and revoke that role from users provisioned with the Application Implementation Consultant role.

Tools Used to Perform Security Tasks

Security tasks are supported by tools within both Oracle Fusion Applications and Oracle Fusion Middleware.

The figure lists the tasks associated with each of the integrated products and pillars of an Oracle Fusion Applications deployment.



Security Setup Tasks: How They Fit Together

Set up security before and after setting up the enterprise with enterprise structures. For some Oracle Cloud Application Services implementations, security setup before enterprise structures setup may not be relevant.

Security setup and administration tasks typically use integrated user interface pages that are provided by the following products.

- Oracle Identity Manager (OIM)
- Oracle Authorization Policy Manager (APM)
- Oracle Fusion Human Capital Management (HCM) products
- Oracle Application Access Control Governor (AACG) in Oracle Enterprise Governance, Risk and Compliance (GRC)

To define data security, administrators and implementation users additionally access integrated user interfaces provided by several products, including the following.

- Oracle Fusion Global Human Resources
- Oracle Fusion Middleware Extensions for Applications (FND)
- Oracle Fusion General Ledger (GL)

- Supplier Portal

Manage users and enterprise role hierarchies in OIM. Manage roles, including duty roles, in APM. Perform supplier role setup tasks for trading partner security in Supplier Portal. Application administrators perform user and role provisioning tasks within applications such as HCM, General Ledger, and Supplier Portal.

Initial Security Setup

The following table shows initial security setup tasks in a likely order, as well as the conditions and purposes of the tasks and where in the user interface these tasks are performed.

Task	Condition	Purpose	Performed In
Create Implementation Users	The predefined Oracle Fusion Applications super user or Oracle Cloud administrator user is generally not the user who will be setting up your enterprise	Create user accounts for implementation users.	OIM
Create Data Role for Implementation Users	The predefined Application Implementation Consultant role access may be too broad	Create a View All data role, such as a View All Financials Application Administrator data role. This data role is based on the Financials Application Administrator job role and combines the entitlements that have been granted to that role with unrestricted access to data on the secured objects that the role is authorized to access.	HCM
Provision Roles to Implementation Users	An implementation user has been created with the Create Implementation Users task	Provision implementation users with roles, such as Application Implementation Consultant, IT Security Manager, and product family Application Administrator job or data roles.	OIM
Revoke Data Role from Implementation Users	None	Revoke any View All data roles after setup is complete.	OIM

Security Setup During Enterprise Setup

When setting up the enterprise with structures such as business units, data roles are automatically generated that inherit job roles based on data role templates. Data roles also can be generated based on HCM security profiles. Data role templates and HCM security profiles enable defining the instance sets specified in data security policies.

Additional Security Setup After Enterprise Setup

An HCM application administrator or application implementation consultant sets up enterprise structures, such as business units and ledgers, using Define Common Application Configuration activities. Basic enterprise structures may already be set up by Oracle in some Oracle Cloud Application Services implementations. After the enterprise has been set up, you can proceed with the following security setup tasks.

The following table shows the tasks in a likely order, as well as the conditions and purposes of the tasks and in which user interface pages these tasks are performed.

Task	Condition	Purpose	Performed In
Import Worker Users	Users or workers are in legacy applications.	If your enterprise has users in legacy applications, use a data load process such as Initiate HCM Spreadsheet Load to import user identities from legacy applications. If there are no legacy users, user accounts are created when workers are imported by performing the Import Workers task in HCM.	OIM
Import Partner Users	• CRM is provisioned • Partner users are in legacy applications	If your enterprise has partner users in legacy applications, use a data load process to import partner identities from legacy applications.	OIM
Manage Job Roles	None	Manage job and abstract (enterprise) roles.	OIM
Manage Duties	None	Manage duty (application) roles and provision to job roles.	APM
Manage Application Access Controls	None	Manage segregation of duties policies.	AACG
Manage Data Access Sets	GL is provisioned.	Define access sets for ledgers and ledger sets.	GL
Manage Segment Security	GL is provisioned.	Manage accounting flexfield segment security rules.	GL
Manage Data Security Policies	Product families other than HCM are provisioned.	Manage data security grants to roles.	APM
Manage Role Templates	None	Manage templates to automatically create or update data roles based on a dimension such as business unit.	APM

Manage Encryption Keys	Oracle Fusion Payments is provisioned.	Create or edit encryption keys held in Oracle Wallet. Encryption keys are used to secure personally identifiable information (PII) attributes.	Payments
Manage Supplier User Roles	Supplier Portal in Procurement is provisioned and requires trading partner security.	Manage roles that can be provisioned to supplier users.	Supplier Portal or Sourcing
Manage Supplier User Role Usages	Supplier Portal in Procurement is provisioned and requires trading partner security.	Manage the supplier roles that can be provisioned by supplier users, and set default roles for Supplier Portal or Sourcing, based on the set of supplier roles that are defined by performing the Manage Supplier User Roles task.	Supplier Portal or Sourcing

Getting Started with an Implementation: Overview

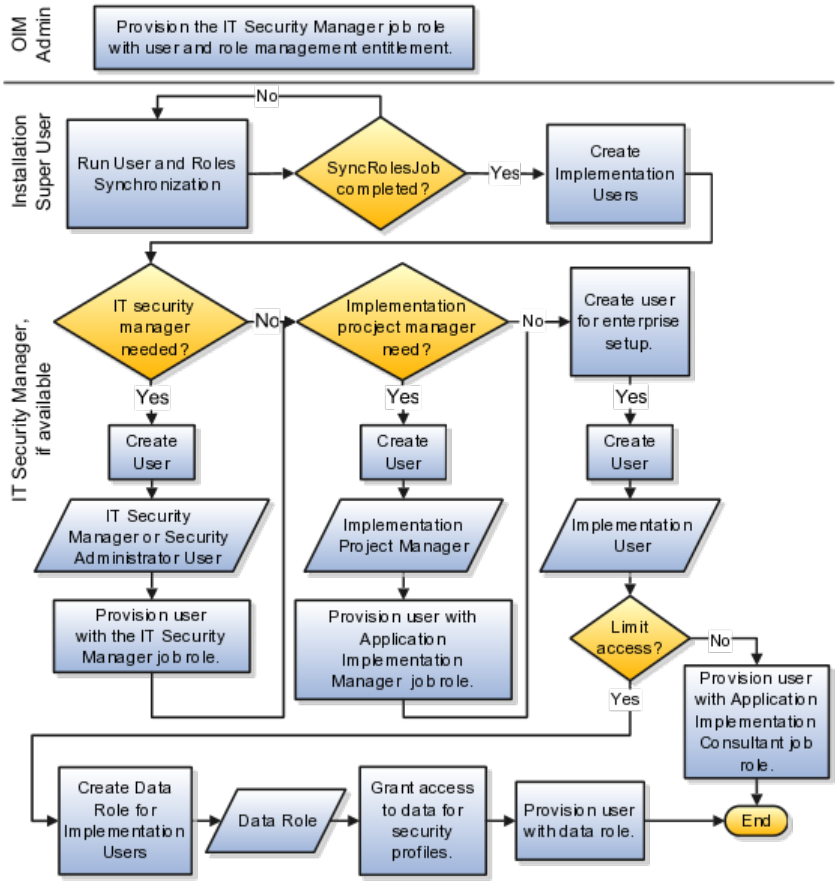
To start an Oracle Fusion Applications implementation, you must set up one or more initial users using the super user that was created during installation and provisioning of the Oracle Fusion Applications environment, or using the initial administrator user provided by Oracle for Oracle Cloud Application Services implementations. Because Oracle Fusion Applications is secure as delivered, the process of enabling the necessary setup access for initial users requires several specialized steps when getting started with an implementation.

The following high level steps are required for starting an implementation.

1. If you are not starting an Oracle Cloud Application Services implementation, sign into Oracle Identity Manager (OIM) as the OIM Administration users and provision the IT Security Manager job role with roles for user and role management. This enables the super user account, which is provisioned with the IT Security Manager job role, to create implementation users.
2. For starting all implementations, sign in as the user with initial access: either the Oracle Fusion Applications installation super user or the initial Oracle Cloud Application Services administrator user.
3. Select an offering to implement, and generate the setup tasks needed to implement the offering.
4. Perform the following security tasks:
   a. Synchronize users and roles in the Lightweight Directory Access Protocol (LDAP) store with HCM user management by using the Run User and Roles Synchronization Process task.
   b. Create an IT security manager user by using the Create Implementation Users task.
   c. Provision the IT security manager with the IT Security Manager role by using the Provision Roles to Implementation Users task.

5. As the newly created IT security manager user, sign in to Oracle Fusion Applications and set up at least one implementation user for setting up enterprise structures.
   a. Create an implementation user by using the Create Implementation Users task.
   b. Provision the implementation user with the Application Implementation Manager job role or the Application Implementation Consultant job role by using the Provision Roles to Implementation Users task. The Application Implementation Consultant job role inherits from all product-specific application administrators and entitles the necessary View All access to all secured object.
   c. Optionally, create a data role for an implementation user who needs only the limited access of a product-specific Application Administrator by using the Create Data Role for Implementation Users. Then assign the resulting data role to the implementation user by using the Provision Roles to Implementation Users task.

The figure shows the task flow from provisioning the IT Security Manager job role with the user and role management entitlement to creating and provisioning implementation users for enterprise setup.



Initial Security Administration: Critical Choices

After installation and provisioning, and before setting up enterprise structures and implementing projects, you must establish required entitlement for the

super user account and at least one implementation user to proceed with the implementation. Once initial enterprise structure setup is complete, additional users may be created through processes available in Human Capital Management (HCM).

Initial security administration consists of the following.

- Preparing the IT Security Manager job role
- Synchronizing users and roles from Lightweight Directory Access Protocol (LDAP) with HCM
- Creating implementation users
- Optionally creating data roles for implementation users
- Provisioning implementation users with roles

Once the first implementation project begins and the enterprise work structure is set up, use standard user and security management processes such as the Manage Users task to create and manage additional users. Do not use the Create Implementation Users task after your enterprise has been set up.

Preparing the IT Security Manager Job Role

Initially the super user is not provisioned to manage users and roles.

You must add the following Oracle Identity Management (OIM) roles to the IT Security Manager job role's role hierarchy to enable the super user to create one or more initial implementation users.

- Identity User Administrators
- Role Administrators

Additionally, you must assign the Xellerate Users organization to the IT Security Manager role.

Synchronizing Users and Roles from LDAP

After configuring an offering and setting up the task lists for implementation, the Run User and Roles Synchronization Process task is available to the super user for synchronizing users and roles in the LDAP store with Oracle Fusion Human Capital Management (HCM).

Defining Initial Implementation Users

The super user is provisioned with roles that provide broad access to Oracle Fusion Middleware and Oracle Fusion Applications administration, and is not suitable as an implementation user in most enterprises. The super user should define at least one implementation user, which consists of creating the user account and provisioning it with at least the Application Implementation Consultant and Application Implementation Manager job roles.

As a security guideline, define an IT security manager user who in turn defines one or more implementation users to set up enterprise structures. The IT security manager users can provision the implementation user with the Application Implementation Consultant role, which entitles access to all enterprise structures.

Or the IT security manager can create a data role that restricts access to enterprise structures of a specific product and provisioning that role.

Depending on the size of your implementation team, you may only need a single implementation user for security administration, implementation project management, enterprise structures setup, and application implementation. That single user must then be provisioned with all indicated roles, and therefore broad access.

Creating Implementation Users

The super user creates one or more implementation users by performing the Create Implementation Users task.

Note

This initial implementation user is a user account created in Oracle Identity Management only, specifically for setting up enterprise structures, and is not related to a real person or identity such as a user defined in HCM.

Creating Data Roles for Implementation Users

As an alternative to provisioning an implementation user with the Application Implementation Consultant role to access all enterprise structures, you may need implementation users with access restricted to enterprise structures for specific products. In this case, use the Create Data Roles for Implementation Users task to create a data role based on a job role with less broad access, such as the HCM Application Administrator job role.

Provisioning Roles to Implementation Users

After creating an implementation user, you must provision the user with one or more roles by performing the Provision Roles to Implementation Users task.

For example, assign a role to the implementation user that provides the access necessary for setting up the enterprise. Depending on need, provision to the implementation user the predefined Applications Implementation Consultant role or a product family-specific administrator data role, such as a data role based on the predefined Financials Applications Administrator.

Caution

The Application Implementation Consultant has broad access. It is a very useful role for experimentation or setting up a pilot environment, but may not be suitable for implementation users in a full implementation project.

Initial Security Administration: Worked Example

This example illustrates initial security administration after having installed and provisioned an Oracle Fusion Applications environment.

In Oracle Fusion Applications, you manage users and security through Oracle Fusion Human Capital Management (HCM) user management flows, which are included in each of the offering task lists. However, the HCM task flows

require that enterprise structures have been set up, and yet to add users who can set up enterprise structures you need to have set up HCM. Therefore, you need to create one or more initial implementation users who are responsible for providing the following.

- Users and their applications security management
- Implementation project management
- Initial enterprise structures management

The following table summarizes key decisions for this scenario.

Decision	In this Example
How to sign in to Oracle Fusion Applications for the first time	Use the super user account that was created when installing and provisioning Oracle Fusion Applications (for example, FAADMIN).
How to ensure that the roles and users in the Lightweight Directory Access Protocol (LDAP) store match what is available for selection when defining implementation users	Perform the Run User and Roles Synchronization Process task.
How to create a first implementation user	Prepare the IT Security Manager job role for user and role management so the super user and any other user provisioned with the IT Security Manager job role can manage users and roles.
How to establish security administration users	Define an IT security manager user provisioned with the IT Security Manager job role.
How to establish an implementation user with access to set up enterprise structures	Define an implementation user provisioned with the Application Implementation Consultant job role.

You create an initial implementation user by performing the following tasks.

1. The Oracle Identity Management System Administrator user provisions the IT Security Manager job role with roles for user and role management.
2. The Oracle Fusion Applications super user synchronizes LDAP users with HCM user management so that users can be provisioned with roles through HCM.
3. The Oracle Fusion Applications super user performs the Create Implementation Users task to create one or more IT security manager and administrator users provisioned with security administrative entitlement.
4. The IT Security Manager user signs in to Oracle Fusion Applications and performs the Create Implementation Users task to create implementation managers and users.
5. The IT Security Manager user provisions implementation users for enterprise structure setup.

Note

The following tasks assume that the super user has configured an offering and set up task lists. When not following a task flow within an activity, you can find tasks in **Navigator > Tools > Setup and Maintenance > All Tasks** . Search for the task and click its **Go to Task** icon in the search results.

Preparing the IT Security Manager Role

The super user that was created when installing and provisioning Oracle Fusion Applications (for example, FAADMIN), or the initial administrator user provided by Oracle for Oracle Cloud Application Services, has all necessary access for implementing Oracle Fusion Applications and administering security. This access is provided by the following roles:

- Application Implementation Consultant
- IT Security Manager

Neither of these roles provides access needed for creating and managing Oracle Fusion Applications users. Therefore, you must add the following two OIM roles to the IT Security Manager role:

- Identity User Administrators
- Role Administrators

The following procedure is prerequisite to an IT security manager or administrator creating an initial one or more implementation users.

1. While signed into Oracle Identity Manager as the OIM System Administrator user, click the **Administration** link in the upper right of the Oracle Identity Manager.

   This accesses the Welcome to Identity Manager Delegated Administration menu.

2. In the Roles list of tasks, click **Advanced Search - Roles**. Search for the Identity Users Administrators role by entering the role name in **Display Name** and clicking **Search**.

   In the Search Results, click the role's Display Name.

3. On the Hierarchy tab, select **Inherits From** and click **Add**.

4. In the Add Parent Role to: IDENTITY USER ADMINISTRATORS window, select the role category: Common - Job Roles and add the IT Security Manager.

   Click the arrow icon to show the list of available roles. Select IT Security Manager and move it to the **Roles to Add** list. Click **Save**.

5. Search for the Role Administrators role, and repeat steps 1 to 4 to add that role to the IT Security Manager role's role inheritance.

6. Assign the IT Security Manager role to the Xellerate Users organization.
   a. In the Welcome to Identity Manager Delegated Administration menu (see step 1, above), in the Organizations list of tasks, click **Advanced Search - Organizations**.

   b. Search for the Xellerate Users organization by entering Xellerate Users in **Display Name** and clicking **Search**.

   c. In the Search Results, click the organization's Display Name. The Xellerate Users page appears.

d. Click the **Administrative Roles** link in the row of links above the Xellerate Users.

e. In **Filter By Role Name** of the Details window, enter the following string:

```
*IT_SECURITY_MANAGER*
```

Click **Find**.

f. Enable Read, Write, Delete, and Assign.

g. Click **Assign**.

h. Click **Confirm**.

Synchronizing Users and Roles from LDAP

Lightweight Directory Access Protocol (LDAP) must be synchronized with HCM user management so that users can be provisioned with roles through HCM.

1. Sign in to Oracle Fusion Applications using the super user's user name (for example FAADMIN) and password.

   If you do not know the super user name and password, check with your system administrator or the person who installed Oracle Fusion Applications. For more information about account creation in Oracle Fusion Applications provisioning, see the Oracle Fusion Applications Installation Guide.

2. Perform the Run User and Roles Synchronization Process task by clicking **Submit** in the Process Details page.

   The Retrieve Latest LDAP Changes process takes some time to complete the first time it is run.

3. Monitor completion of the Retrieve Latest LDAP Changes process from **Navigator > Tools > Scheduled Processes** before continuing with creating implementation users.

Defining an IT Security Manager User

The super user has broad access to Oracle Fusion Middleware and Oracle Fusion Applications administration. Due to this broad access, your enterprise needs users dedicated to managing users and applications security, such as an IT security manager user.

1. While signed in as the Oracle Fusion Applications super user, access the Create Implementation Users task and create an IT security manager.

   The Oracle Identity Manager appears.

2. Click **Create User**.

   For details, see the Creating Users section in the Oracle Fusion Middleware User's Guide for Oracle Identity Manager.

3. Provide the following attributes:

Attribute	Value	Example
Last name	<any valid string>	Smith
Organization	Xellerate Users	N/A
User type	Non Worker	N/A
User login	<any valid string>	IT_SECURITY_MANAGER
Login password	<any valid string>	SeKur1TyPa$$w0Rd

Note

In Oracle Fusion Applications, an implementation user is a user account created in OIM only, specifically for implementation tasks, and is not related to a real person or identity such as a user defined in HCM.

4. Click **Save**.
5. On the Roles tab in the IT_SECURITY_MANAGER user creation task flow, click **Assign**.
6. In the Add Role window, search for the IT Security Manager role and click **Add**.

Defining an Implementation User for Enterprise Structures Setup

1. Sign in to Oracle Fusion Applications using the IT security manager user's name and password.
2. Create and provision an implementation user using the same task flow as for creating the IT security manager user in the previous section, except provision the following roles.
   - Application Implementation Manager
   - Application Implementation Consultant

Note

For an implementation to begin, at least one user must be provisioned with the Application Implementation Manager role, and another or the same user must be provisioned with the Application Implementation Consultant role. The Application Implementation Consultant has broad access to set up all enterprise structures.

Defining Security After Enterprise Setup: Points to Consider

After the implementation user has set up the enterprise, further security administration depends on the requirements of your enterprise.

The Define Security activity within the Information Technology (IT) Management business process includes the following tasks.

- Import Worker Users
- Import Partner Users
- Manage Job Roles
- Manage Duties
- Manage Application Access Controls

If no legacy users, user accounts, roles, and role memberships are available in the Lightweight Directory Access Protocol (LDAP) store, and no legacy workers are available in Human Resources (HR), the implementation user sets up new users and user accounts and provisions them with roles available in the Oracle Fusion Applications reference implementation.

If no legacy identities (workers, suppliers, customers) exist to represent people in your enterprise, implementation users can create new identities in Human Capital Management (HCM), Supplier Portal, and Customer Relationship Management (CRM) Self Service, respectively, and associate them with users.

Before Importing Users

Oracle Identity Management (OIM) handles importing users.

If legacy employees, contingent workers, and their assignments exist, the HCM Application Administrator imports these definitions by performing the Initiate HCM Spreadsheet Load task. If user and role provisioning rules have been defined, the Initiate HCM Spreadsheet Load process automatically creates user and role provisioning requests as the workers are created.

Once the enterprise is set up, performing the Initiate HCM Spreadsheet Load task populates the enterprise with HR workers in records linked by global user ID (GUID) to corresponding user accounts in the LDAP store. If no user accounts exist in the LDAP store, the Initiate HCM Spreadsheet Load task results in new user accounts being created. Worker email addresses as an alternate input for the Initiate HCM Spreadsheet Load task triggers a search of the LDAP for user GUIDs, which may perform more slowly than entering user names.

In the security reference implementation, the HCM Application Administrator job role hierarchy includes the HCM Batch Data Loading Duty role, which is entitled to import worker identities. This entitlement provides the access necessary to perform the Initiate HCM Spreadsheet Load task in HCM.

Note

The Import Person and Organization task in the Define Trading Community Import activity imports the following resources, creates users, and links the resources to users for use in CRM.

- Internal employees
- Contingent workers
- External partner contacts
- Partner companies
- Legal entities

- Customers
- Consumers

If role provisioning rules have been defined, the Import Person and Organization task automatically provisions role requests as the users are created.

Import Users

If legacy users (identities) and user accounts exist outside the LDAP store that is being used by the Oracle Fusion Applications installation, the IT security manager has the option to import these definitions to the LDAP store by performing the Import Worker Users and Import Partner Users tasks.

If no legacy users or user accounts can be imported or exist in an LDAP repository accessible to Oracle Identity Management (OIM), the IT security manager creates users manually in OIM or uses the Initiate HCM Spreadsheet Load task to create users from imported HR workers.

Once users exist, their access to Oracle Fusion Applications is dependent on the roles provisioned to them in OIM or Human Capital Management. Use the Manage HCM Role Provisioning Rules task to define rules that determine what roles are provisioned to users.

Importing user identities from other applications, including other Oracle Applications product lines, is either a data migration or manual task. Migrating data from other Oracle Applications includes user data. For more information about importing users, see the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.

In the security reference implementation, the IT Security Manager job role hierarchy includes the HCM Batch Data Loading Duty and the Partner Account Administration Duty. These duty roles provide entitlement to import or create users. The entitlement Load Batch Data provides the access necessary to perform the Import Worker Users task in OIM. The entitlement Import Partner entitlement provides the access necessary to perform the Import Partner Users task in OIM.

Manage Job Roles

Job and abstract roles are managed in OIM. This task includes creating and modifying job and abstract roles, but not managing role hierarchies of duties for the jobs.

Note

Manage Job Roles does not include provisioning job roles to users. Provisioning users is done in OIM, HCM, CRM or Oracle Fusion Supplier Portal.

Roles control access to application functions and data. Various types of roles identify the functions performed by users.

The Oracle Fusion Applications security reference implementation provides predefined job and abstract roles. In some cases, the jobs defined in your

enterprise may differ from the predefined job roles in the security reference implementation. The predefined roles and role hierarchies in Oracle Fusion may require changes or your enterprise may require you to create new roles. For example, you need a job role for a petty cash administrator, in addition to an accounts payable manager. The security reference implementation includes a predefined Accounts Payable Manager, and you can create a petty cash administrator role to extend the reference implementation.

In the security reference implementation, the IT Security Manager job role hierarchy includes the Enterprise Role Management Duty role, which is entitled to manage job and abstract roles (the entitlement is Manage Enterprise Role). This entitlement provides the access necessary to perform the Manage Job Roles task in OIM.

Manage Duties

A person with a job role must be able to perform certain duties. In the Oracle Fusion Applications security reference implementation, enterprise roles inherit duties through a role hierarchy. Each duty corresponds to a duty role. Duty roles specify the duties performed within applications and define the function and data access granted to the enterprise roles that inherit the duty roles.

Managing duties includes assigning duties to job and abstract roles in a role hierarchy using Authorization Policy Manager (APM). If your enterprise needs users to perform some actions in applications coexistent with Oracle Fusion applications, you may wish to remove the duty roles that enable those actions. For details about which duty roles are specific to the products in an offering, see the Oracle Fusion Applications Security Reference Manual for each offering.

OIM stores the role hierarchy and the spanning of roles across multiple pillars or logical partitions of applications.

In cases where your enterprise needs to provide access to custom functions, it may be necessary to create or modify the duty roles of the reference implementation.

Tip

As a security guideline, use only the predefined duty roles, unless you have added new applications functions. The predefined duty roles fully represent the functions and data that must be accessed by application users and contain all appropriate entitlement. The predefined duty roles are inherently without segregation of duty violations of the constraints used by the Application Access Controls Governor.

In the security reference implementation, the IT Security Manager job role hierarchy includes the Application Role Management Duty role, which is entitled to manage duty roles (the entitlement is Manage Application Role). This entitlement provides the access necessary to perform the Manage Duties task in APM.

Note

Product family administrators are not entitled to create role hierarchies or manage duty roles and must work with the IT security manager to make changes

such as localizing a duty role to change a role hierarchy. Setup for localizations is documented in HCM documentation.

Manage Application Access Controls

Prevent or limit the business activities that a single person may initiate or validate by managing segregation of duties policies in the Application Access Controls Governor (AACG) .

Note

In AACG, segregation of duties policies are called access controls or segregation of duties controls.

In the security reference implementation, the IT Security Manager job role hierarchy includes the Segregation of Duties Policy Management Duty role, which is entitled to manage segregation of duties policies (the entitlement is Manage Segregation of Duties Policy). This entitlement provides the access necessary to perform the Manage Application Access Controls task in AACG.

Defining Data Security After Enterprise Setup: Points to Consider

After the implementation user has set up the enterprise, further security administration depends on the requirements of your enterprise.

The Define Data Security activity within the Information Technology (IT) Management business process includes the following tasks.

- Manage Data Access Sets
- Manage Segment Security
- Manage Role Templates
- Manage Data Security Policies
- Manage Encryption Keys

These tasks address data security administration. For information on using the user interface pages for setting up and managing data security, see the Oracle Fusion Middleware Administrator's Guide for Authorization Policy Manager (Oracle Fusion Applications edition).

Note

The Manage Data Role and Security Profiles task, and all other HCM security profile setup tasks are documented in Human Capital Management (HCM) documentation.

Manage Data Access Sets

Data access sets define a set of access privileges to one or more ledgers or ledger sets.

The information on ledgers that are attached to data access sets are secured by function security. Users must have access to the segment values associated with the data access sets to access the corresponding GL account.

In the security reference implementation, the IT Security Manager job role hierarchy includes the Data Access Administration Duty role, which is entitled to manage data access sets (the entitlement is Define General Ledger Data Access Set). This entitlement provides the access necessary to perform the Manage Data Access Sets task in General Ledger.

Manage Segment Security

Balancing or management segment values can secure data within a ledger.

Segment values are stored in GL_ACCESS_SET_ASSIGNMENTS and secured by restrictions, such as Exclude, on parameters that control the set of values that a user can use during data entry.

In the security reference implementation, the IT Security Manager job role hierarchy includes the Application Key Flexfield Administration Duty role, which is entitled to manage application key flexfields (the entitlement is Manage Application Key Flexfield). This entitlement provides the access necessary to perform the Manage Segment Security task in General Ledger.

Manage Role Templates

Data role templates automatically create or update data roles based on dimensions such as business unit. As an enterprise expands, data role templates trigger replication of roles for added dimensions. For example, when creating a new business unit, a data role template generates a new Accounts Payables Manager data role based on the Financials Common Module Template for Business Unit Security data role template.

In the security reference implementation, the IT Security Manager job role hierarchy includes the Application Role Management Duty role, which is entitled to manage data role templates (the entitlement is Manage Role Template). This entitlement provides the access necessary to perform the Manage Role Templates task in APM.

Manage Data Security Policies

Data security grants provisioned to roles are data security policies. The security reference implementation provides a comprehensive set of predefined data security policies and predetermined data security policies based on data role templates.

Data security policies are available for review in Authorization Policy Manager (APM). Data security policies are implemented by grants stored in Oracle Fusion Data Security (FND_GRANTS).

Data security policies secure the database resources of an enterprise. Database resources are predefined applications data objects and should not be changed. However, for cases where custom database resources must be secured objects, the IT security manager is entitled to manage database resources and create new data security policies.

Warning

Review but do not modify HCM data security policies in APM except as a custom implementation. Use the HCM Manage Data Role And Security Profiles task to generate the necessary data security policies and data roles.

In the security reference implementation, the IT Security Manager job role hierarchy includes the Application Role Management Duty role, which is entitled to manage data security policies (the entitlement is Manage Data Security Policy). This entitlement provides the access necessary to perform the Manage Data Security Policies task in APM.

Manage Encryption Keys

Create or edit encryption keys held in Oracle Wallet to secure Personally Identifiable Information (PII) attributes This task is only available when Payments is implemented.

In the security reference implementation, the IT Security Manager job role hierarchy includes the Payments Data Security Administration Duty role, which is entitled to manage encryption keys that secure PII (the entitlement is Manage Wallet). This entitlement provides the access necessary to perform the Manage Encryptions Keys task in Payments.

Defining Trading Partner Security After Enterprise Setup: Points to Consider

Trading partner access can be secured with user roles and user role usages for suppliers.

Trading Partner Security tasks within the Information Technology (IT) Management business process are:

- Manage Supplier User Roles
- Manage Supplier User Role Usages

Manage Supplier User Roles

This task manages roles that the supplier administrator can provision to supplier users, and is only available when the Supplier Portal or Sourcing are implemented.

In the security reference implementation, the IT Security Manager job role hierarchy includes the User Management Duty role, which is entitled to create and manage users (the entitlement is Manage User Principal). This entitlement provides the access necessary to perform the Create Implementation Users task in OIM.

In the security reference implementation the IT Security Manager job role hierarchy includes the Supplier User Role Management Duty role, which is entitled to manage supplier user roles (the entitlement is Manage Supplier User

Roles). This entitlement provides the access necessary to perform the Manage Supplier User Roles task in the Supplier Portal or Sourcing.

Manage Supplier User Role Usages

This task manages the set of roles and default roles that supplier users can provision based on the roles that are defined by the Manage Supplier User Roles task.

This task is only available when the Supplier Portal or Sourcing are implemented.

In the security reference implementation, the IT Security Manager job role hierarchy includes the Supplier Portal Configuration Management Duty role, which is entitled to manage supplier user roles (the entitlement is Manage Supplier User Role Usages). This entitlement provides the access necessary to perform the Manage Supplier User Roles Usages task in the Supplier Portal or Sourcing.

Security Tasks After Enterprise Changes: Points To Consider

Various changes to your enterprise require security adjustments.

- New enterprise roles
- Reorganization

Note

Oracle Fusion Applications security does not require security adjustments after HCM changes, such as when a person changes to another job, because their provisioned roles are automatically revoked and recalculated based on role provisioning rules.

New Enterprise Roles

You may be adding new abstract or job roles or both, and the data role templates in your deployment may be generating new data roles as you set up new dimensions.

As a security guideline, adjust your role provisioning rules so these new roles are appropriately provisioned.

Tip

Review data role templates to identify newly generated data roles after enterprise setup changes. For example, the Financials Common Module Template for Business Unit generates new data roles after you create a new business unit. These data roles need to be provisioned.

Reorganization

You may create a new business unit or combine existing business units.

Securing the change may require security tasks including the following.

- Changes to role provisioning rules for new or obsolete data roles.

Top Security Tasks

The top security administration tasks for IT security managers and security administrators are the ones required or most likely necessary in setting up and implementing Oracle Fusion Applications security.

Top security tasks include the following.

- Top initial security setup tasks
- Top tasks for defining security implementation
- Top security administration tasks

Top Initial Security Setup Tasks

The top initial security setup tasks are as follows.

Security task	Importance to managing risk	Frequency	Notes
1. Import Worker Users	Low	Depends on need	
2. Create Implementation Users	Low	Required	Task flow includes provisioning roles to a new implementation user
3. Provision Roles to Implementation Users	High	Optional	Used for provisioning additional roles, such as data roles

Top Tasks for Defining Security Implementation

After reviewing the security reference implementation, as presented in the Security Reference Manual for each offering, the top tasks for defining security implementation are as follows.

Security task	Importance to managing risk	Frequency	Notes
4. Implement predefined data security policies by generating data roles (if appropriate) and HCM security profiles.	High	Depends on need	To understand what data roles are available, review the predefined data role templates and HCM security profiles. Once data roles are generated based on your implementation of data role templates and Human Capital Management (HCM) security profiles, modify or define role

5. Manage Data Security Policies when customizing, such as when adding a database resource (table)	High	Initially or when new database resources needs to be secured	To understand the data security provided by the Oracle Fusion Applications security reference implementation, it is important to review the predefined data security policies.
6. Manage Duties	High	Initially or when new jobs are defined	To understand the Oracle Fusion Applications security reference implementation and the job roles available for provisioning to users, it is important to understand the duty roles inherited by those job roles. As a security guideline, duty roles should not be changed, only their participation in role hierarchies.

Top Security Administration Tasks

The top security administration tasks are as follows.

Security Task	Importance to managing risk	Frequency	Notes
7. Approve User and Role Provisioning Requests	High	Infrequent	Provisioning requests are pre-approved in HCM. This task can be set up to be manual. Approvals are required when provisioning a role in HCM causes a segregation of duties (SOD) violation.
8. Assign User Roles	Low	Never - this task is in Workforce Deployment and performed by HCM roles or when provisioning supplier users in Supplier Portal	The Oracle Fusion Applications security reference implementation provides abstract, job, and data roles available for provisioning to user. Without provisioned roles, users are not authorized to access the portions of Oracle Fusion applications necessary to perform their duties.
9. View segregation of duties (SOD) policy conflicts and violations	High	Infrequent	Significant where reference security implementation changes

FAQs for Security Tasks

How can I view the duties included in a job role?

Use the Manage Duties task to view the duties inherited by a role. To perform this task, you'll use the integrated Authorization Policy Manager.

Each logical partition or pillar contains a collection of application roles representing duties, and function and data security policies carried by those roles.

How do I view the entitlement or policies carried by a job role?

Use the Manage Duties task to view the entitlement carried by the duty roles in a role hierarchy, or policies carried by enterprise roles. To perform this task, you'll use the integrated Authorization Policy Manager.

The Lightweight Directory Access Protocol (LDAP) policy store stores application roles representing duties, and the identity store stores enterprise roles.

How do I change which roles are in a role hierarchy?

Use the Manage Job Roles task to create a hierarchy of enterprise roles. To perform this task, you'll use the integrated Oracle Identity Management UI pages.

Use the Manage Duties task to create a hierarchy of duty roles. To perform this task, you'll use the integrated Authorization Policy Manager.

The Lightweight Directory Access Protocol (LDAP) stores the role hierarchy and the spanning of roles across multiple pillars or logical partitions. The policy store stores duty roles. The identity store stores enterprise roles.

How do I create a hierarchy of roles?

Use the Manage Job Roles task to create a hierarchy of enterprise roles. Use the integrated Oracle Identity Management UI pages to perform this task

User the Manage Duties task to create a hierarchy of applications roles. Use the integrated Authorization Policy Manager to perform this task.

Why would I need to remove duty roles from a role hierarchy?

Some duty roles may enable actions and their associated users interface features that your enterprise does not want users to perform in Oracle Fusion applications.

How do I create a new job role?

Use the following tasks to view the job, abstract, and data roles provisioned to a user.

- Create Job Roles
- Manage Job Roles

Use the integrated Oracle Identity Management UI pages to perform these tasks. The Lightweight Directory Access Protocol (LDAP) identity store stores enterprise roles.

Can I create a new duty role?

Yes, but this should only be necessary if you have extended your Oracle Fusion Applications with new duties involving custom objects or functions that must be secured.

Use the Manage Duties task to create a duty role. To perform this task, you'll use the integrated Authorization Policy Manager.

How can I view the segregation of duties policies respected by a role?

Use the Manage Segregation of Duties Policies task to view segregation of duties policies. Use the integrated Application Access Controls Governor (AACG) in Oracle Enterprise Governance, Risk and Compliance (GRC) to perform this task.

The Oracle Fusion Applications security reference manual (SRM) for each offering documents the segregation of duties (SOD) policies respected within each job role.

How can I view segregation of duties policy violations?

Use the Manage Application Access Controls task to view segregation of duties policy violations carried by the duty roles inherited by a job role. Use the integrated Application Access Controls Governor (AACG) in Oracle Enterprise Governance, Risk and Compliance (GRC) to perform this task.

The Oracle Fusion Applications security reference manual (SRM) for each offering documents the segregation of duties (SOD) policies respected within each job role.

How can I view or change the data security policies carried by job, abstract, and data roles?

Use the Manage Data Security Policies task to view or change data security policies. To perform this task, you'll use the integrated Authorization Policy Manager or data security pages provided by Oracle Fusion Middleware Extensions for Applications (Applications Core).

Oracle Fusion Data Security stores data security policies in the policy store.

How do I create a new data role?

Use the Manage Role Templates task to define which data roles are generated. To perform this task, you'll use the integrated Authorization Policy Manager.

Use the Manage Data Roles and Security Profiles task to define which HCM data roles are generated. To perform this task, you'll use Oracle Fusion Human Capital Management (HCM).

These tasks may trigger the need for revised role provisioning rules to ensure that new data roles are appropriately provisioned to users.

How can I create a new data security policy?

Use the Manage Data Security Policies task to create new data security policies. Data security policies can also be created by generating data roles based on data role templates or HCM security profiles. To perform this task, you'll use the integrated Authorization Policy Manager or data security pages provided by Oracle Fusion Middleware Extensions for Applications (Applications Core).

Oracle Fusion Data Security stores data security policies in the policy store.

How can I view, create, or change a data role template?

Use the Manage Role Templates task to view, create, or change data role templates. Use the integrated Authorization Policy Manager to perform the Manage Role Templates task.

How can I secure a common object such as an attachment category or a profile option?

Use the Manage Data Security Policies task to secure objects. To perform this task, you'll use the integrated Authorization Policy Manager or data security pages provided by Oracle Fusion Middleware Extensions for Applications (Applications Core).

How do I view, create, or update encryption keys used to secure attributes of personally identifiable information?

Use the Manage Encryption Keys task, which is available in Oracle Fusion Payments.

How do I view, create, or update data access sets used to secure ledgers and ledger sets?

Use the Manage Data Access Sets task, which is available in Oracle Fusion General Ledger.

How do I view, create, or update accounting flexfield segment security rules?

Use the Manage Security Segments task, which is available in Oracle Fusion General Ledger.

Why can't a user access a task?

If a user believes a necessary task is missing from their list of tasks, they may need to be provisioned with different or additional roles.

Access is provisioned to users based on their position or job, which consists of the duties performed in that job. Provisioned enterprise roles provide access by means of inherited duty roles.

The duty roles in a role hierarchy carry entitlement to access functions and data. Duty roles are not provisioned directly to users but granted to enterprise roles in a role hierarchy. As a security guideline, refrain from changing the privileges of the duty role's entitlement. If more or less entitlement is required by an enterprise role, change the role hierarchy that defines the enterprise role instead.

Users are generally provisioned with roles based on role provisioning rules. If a user requests being provisioned with a role to access a task, use the security considerations of your enterprise and the roles available in your security reference implementation to determine which roles are appropriate.

How can I tell which roles are provisioned to a user?

Use the following tasks to view the job, abstract, and data roles provisioned to a user.

- Manage Users
- Manage User Principal
- Provision Roles to Implementation Users

Use Human Capital Management and integrated Oracle Identity Management UI pages to perform these tasks. Users, roles, and provisioning information are stored in Lightweight Directory Access Protocol (LDAP) stores.

How can I create a new user?

Use the Manage Users task to create new users. Use Human Capital Management (HCM) pages to perform this task.

When you create a new worker, HCM creates a new user and identity.

The Hire Employee and Add Contingent Worker tasks also result in new user creation requests.

Creating a new user automatically triggers role provisioning requests based on role provisioning rules.

Note

If you are creating new implementation users for setting up your enterprise, use the Create Implementation Users task. Use the integrated Oracle Identity Management UI pages to perform this task.

How do I provision roles to users?

Use the following tasks to provision roles to users.

- Manage Users
- Provision Roles to Implementation Users

The Manage Users task is available in Oracle Fusion Human Capital Management (HCM), Oracle Fusion Customer Relationship Management (CRM) and Oracle Fusion Suppliers.

Implementation users are provisioned through Oracle Identity Management (OIM) when HCM is not setup at the start of the implementation. The Provision Roles to Implementation Users is not needed once implementation is complete. Once HCM is setup, HCM is used to provision roles to non-implementation users by performing the Manage Users task. Human Resources (HR) transaction flows such as Hire and Promote also provision roles.

How do I view an audit log?

Use Oracle Enterprise Manager to view audit logs. Viewing audit logs is an Oracle Fusion Middleware function and not represented by an Oracle Fusion Applications business process model (BPM) task.

In Oracle Cloud Application Services, contact My Oracle Support to enable auditing and request audit reports.

3

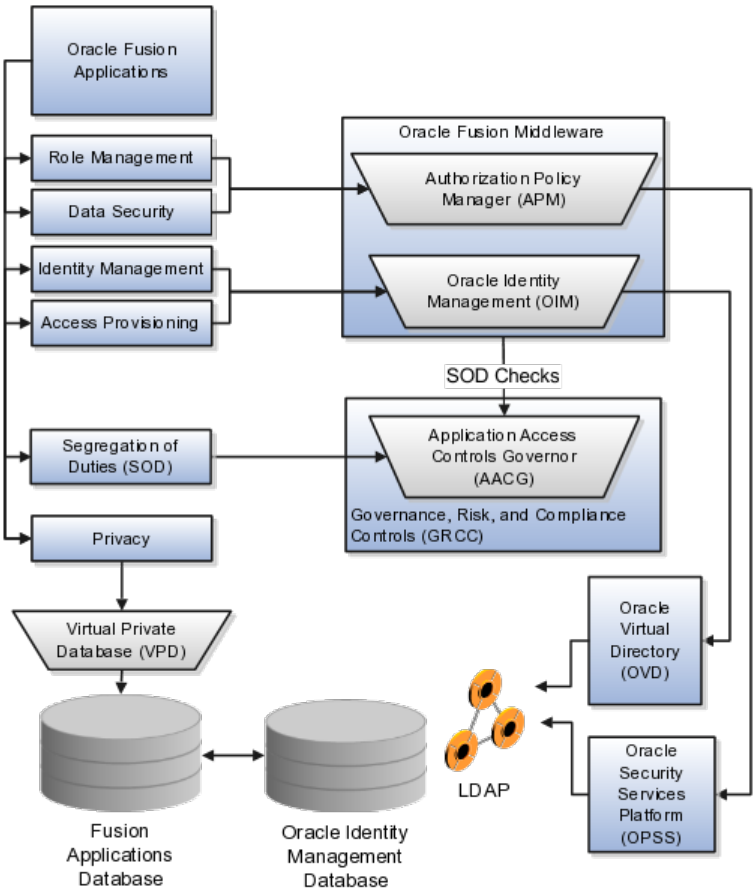
Security Infrastructure

Security Components: How They Fit Together

Users are granted access to various resources using Oracle Identity Management (OIM) and Authorization Policy Manager (APM). Integration with Oracle Enterprise Governance, Risk and Compliance (GRC) supports segregation of duties (SOD).

Oracle Fusion entitlement management secures access to all three tiers at the service-oriented architecture (SOA) layer, which is supported by Oracle Platform Security Services (OPSS). That means that rather than having every application with its own entitlement layer, access is managed as a centralized service shared by all applications.

The figure shows elements of Oracle Fusion Applications security and supporting structures in the Web, application, middle, and data tiers.



Security Components

The following components of an Oracle Fusion Applications deployment participate in security.

Component	Does what?
Oracle HTTP Server (OHS)	Takes all incoming HTTP requests
Oracle Access Manager (OAM)	Performs single sign on (SSO)
Web Gate (OAM component)	Intercepts requests and checks for user credentials
Web Pass (OAM Web server plug-in)	Passes information between the Web server and OAM's Identity Server
OAM Policy Manager	Supports managing single sign on (SSO), and URL-based authentication and authorization policies
Oracle Identity Management (OIM)	Handles user provisioning
Oracle Web Services Manager (OWSM)	Provides infrastructure for Service Oriented Architecture (SOA) and Web services security
OWSM Agent	Enforces SOA and Web services security
OWSM Policy Manager	Supports setting up policy configuration for SOA and Web services security
Oracle Platform Security Services (OPSS)	Provides framework to manage policies, identity, and audit services across the enterprise
Oracle Virtual Directory (OVD)	Virtualizes data sources in Lightweight Directory Access Protocol (LDAP) stores
Identity Governance Framework (IGF)	Manipulates users, groups, and policies in LDAP
Authorization Policy Management (APM)	Supports managing authorization policies
Enterprise Manager (EM)	Supports managing deployed components, services, and applications
Oracle Virtual Private Database (VPD)	Protects personally identifiable information (PII) attributes in the database from unauthorized access by privileged users such as database administrators (DBA)

Note

OAM policies have no relationship with OPSS policies.

Oracle Fusion Applications accesses policies through the services of WebLogic Servers. OPSS populates the Java authorization (JAZN) file with policies for transfer to Lightweight Directory Access Protocol (LDAP) and distribution to applications using WebLogic services.

Security Across Multiple Tiers

The components of the Oracle Fusion Applications security approach span all tiers of a deployment technology stack.

- Data
- Middleware

- Applications
- Web

Installation typically sets up Oracle Fusion Applications in predefined WebLogic Server (WLS) domains. that correspond to product families, such as Financials or Human Capital Management (HCM). A WLS domain is a group of servers working together in the middle tier to serve the Java Platform, Enterprise Edition (Java EE) applications in the applications tier with the data in the database of the data tier.

In the data tier the database manages the data for Oracle Fusion Applications. Data security policies are stored in Oracle Fusion Data Security (FND_GRANTS). Function security policies are stored in the LDAP policy store.

Oracle Internet Directory serves as an LDAP store. If your enterprise is using a different LDAP store, use Oracle Virtual Directory to connect to your LDAP store.

In the middle tier, the WLS contains the business components and user interface faces of the Application Development Framework (ADF) instances that run Oracle Fusion Applications. The middle tier also contains other essential components of an Oracle Fusion Applications deployment that are relevant to security.

- Enterprise Scheduler Services for executing processes
- Oracle WebCenter for managing tags, Watchlists, and Oracle Fusion Search
- Service Oriented Architecture for managing Web services
- Oracle WebCenter Content for managing documents and attachments
- Oracle Identity Manager (OIM) for user provisioning
- Oracle Access Manager (OAM) for authentication and authorization
- Oracle Business Intelligence Foundation Suite for Oracle Applications (OBIFA) and BI Publisher for analytics and reports

All of these components use OPSS to communicate with the applications and Web tiers. OPSS controls abstractions of the pages and widgets that appear in Oracle Fusion applications

Authorization Policy Management defines entitlements using OPSS. LDAP such as Oracle Internet Directory repositories store job roles and users. Oracle Identity Management manages job roles and users.

In the applications tier, Enterprise Manager handles the functional setup and features of your deployment.

In the Web tier, Oracle WebCache, the HTTP Server, and load balancers manage client interactions.

Setup and Runtime Components

The following components must be present at setup and runtime.

- Oracle Database
  - Oracle Text
  - PL/SQL
  - SQL*Loader
  - Oracle Data Integrator (ODI)
- Oracle Database Enterprise Edition
- Oracle Identity Management
  - Identity Governance Framework (IGF)
- WebLogic Server and selected subcomponents
  - Application Development Framework (ADF)
  - ADF Data Visualizations (DVT)
  - Groovy (in ADF business components (ADFbc))
  - Java Architecture for XML Binding (JAXB)
  - Java API for XML Web Services (JAX-WS)
  - Java Transaction API (JTA)
  - Service Component Architecture (SCA)
- SOA Suite and business process management (BPM) Suite selected components
  - Approval Management System (AMX)
  - Business Process Execution Language (BPEL)
  - Business Rules
  - Oracle Enterprise Scheduler
  - Events Delivery Network (EDN)
  - Oracle Content Server (using Oracle WebCenter Framework) with full Oracle WebCenter Content suite
  - Oracle Human Workflow
  - Oracle Mediator
  - Oracle Web Services Manager (OWSM)
  - Oracle WebCenter Framework
- Oracle Single Sign-On Server
- Oracle Virtual Directory

- Oracle Business Intelligence Foundation Suite for Oracle Applications (OBIFA) selected components
  - BI Publisher, including Marketing Segmentation Server
  - Oracle BI Answers
  - Oracle BI Dashboards
  - Oracle BI Delivers
  - Oracle BI Presentation Server
  - Oracle BI Server
- Other components
  - Extended Spread Sheet Database (ESSbase)
  - Oracle Real-Time Decisions (RTD)
  - Enterprise Crawl and Search Framework (ECSF)
  - Any LDAP server (such as, but not limited to, Oracle Internet Directory (OID)).

Note

OID is the LDAP that supports provisioning by default, but Oracle Fusion Applications supports third-party servers directly.

For more information about security in the middle tier, see the Oracle Fusion Middleware Security Overview and the Oracle Fusion Middleware Security and Administrator's Guide for Web Services.

Access Components: Explained

Access components safeguard against unauthorized use at all levels of an Oracle Fusion Applications deployment infrastructure.

Users and provisioning components illustrate how access components interact in an Oracle Fusion Applications deployment.

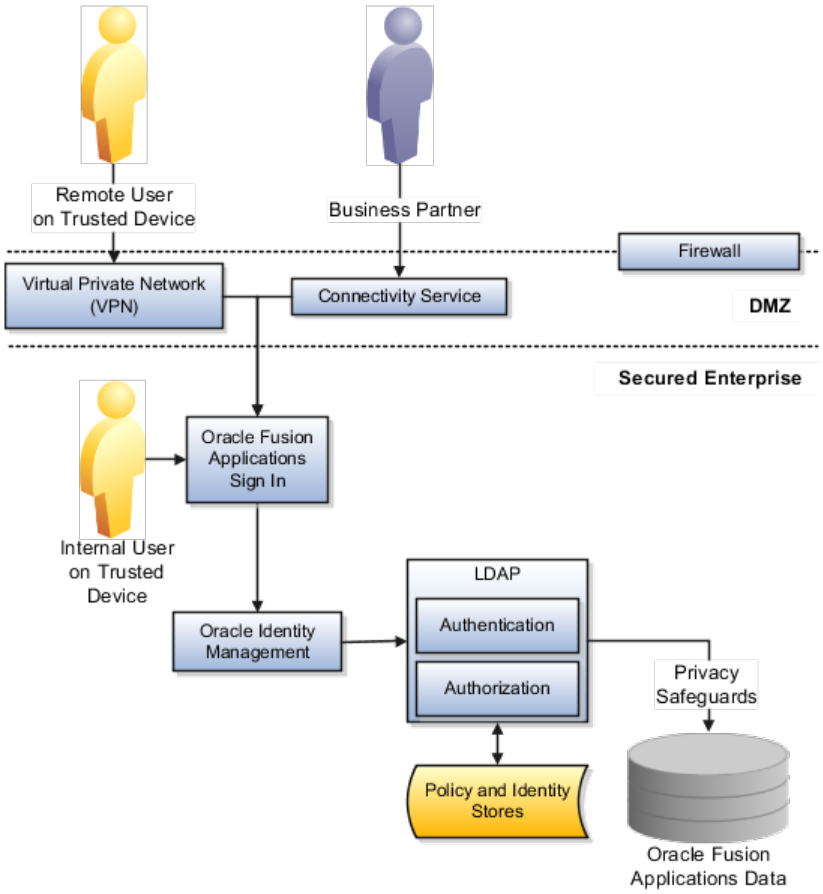
Users

Access components support securing all types of users.

- Internal users on trusted devices
- Remotely located users on trusted devices

- Partners
- Web site users

The following graphic shows Oracle Fusion Applications running on the Web services of Oracle Fusion Middleware and subjecting internal and external users to authentication and authorization as defined by the security policies and identities stored in a Lightweight Directory Access Protocol (LDAP) store. Access to sensitive data is further protected by safeguards such as Oracle Database Vault and Oracle Virtual Directory.



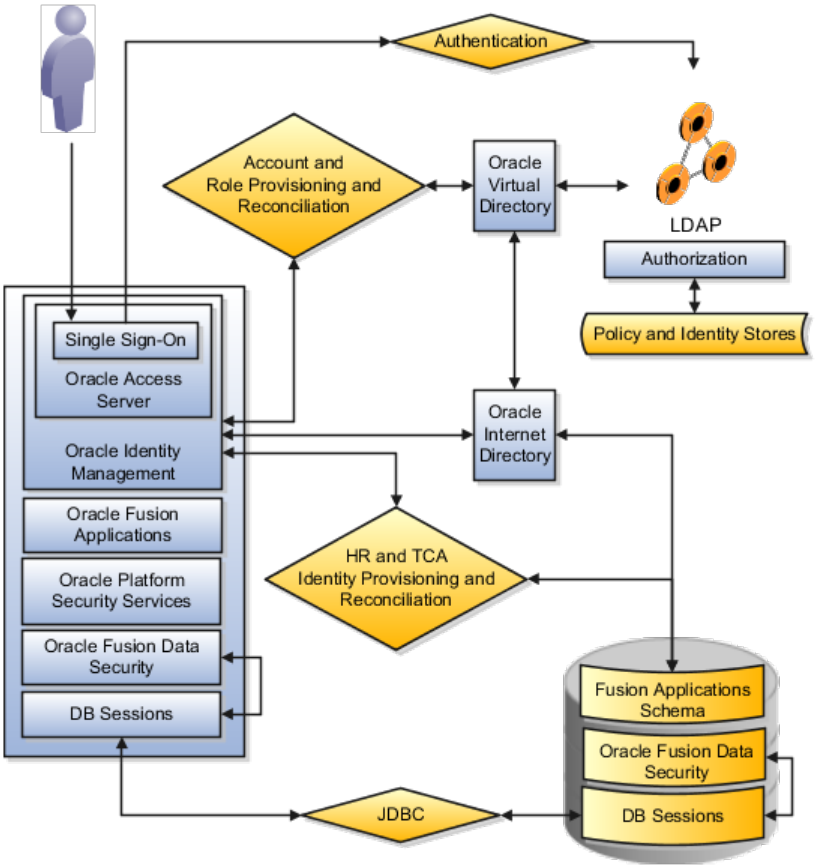
Note

Non-repudiation is handled either through audit trails within Oracle Fusion Applications or through Oracle Web Services Management (OWSM) support for signatures using WebServer security.

Provision Components

Provisioning components additionally safeguard against unauthorized access.

The following diagram shows Oracle Fusion Applications provisioning and reconciliation for accounts, roles, and HR and Oracle Fusion Trading Community Model identity. User and account provisioning uses Oracle Virtual Directory. Oracle Internet Directory is an LDAP repository.



Regulatory Frameworks in Oracle Fusion Applications Security: How They Are Applied

Oracle Fusion Applications security supports compliance with security regulations.

Settings That Affect How Security Regulations Are Applied

The American National Standards Institute (ANSI) standard RBAC (role-based access control) enables efficient compliance with regulations. For specific regulations, features such as personally identifiable information (PII) protections, encryption, and segregation of duties controls provide compliance support.

How Security Regulations Are Addressed

Various features of Oracle Fusion Applications security and the Oracle Enterprise Governance, Risk and Compliance (GRC) suite of products support compliance with security regulations.

Regulations

Oracle Fusion Applications products adhere to or support compliance with the following mandates.

Regulation	Addressed in Oracle Fusion Applications
Gramm-Leach-Bliley Act (GLBA)	Oracle Virtual Private Database (VPD), encryption, and masking to protect clones of production data
Sarbanes - Oxley Act (SOX)	Segregation of duties controls
State regulations such as California SB 1386	VPD, encryption, and masking to protect clones of production data
Payment Card Industry Data Security Standard (PCI-DSS)	VPD, encryption, and masking to protect clones of production data
Health Insurance Portability and Accountability Act (HIPAA)	VPD, encryption, and masking to protect clones of production data
EU Data Protection Directive	VPD, encryption, and masking to protect clones of production data

Oracle Fusion Applications protects PII with VPD, Transparent Data Encryption (TDE) and encryption APIs. Oracle Fusion Applications masks production data using Oracle Data Masking. Network security provides encryption in transit. Oracle Application Access Control Governor provides segregation of duties protections.

Oracle Enterprise Governance, Risk and Compliance (GRC)

Administrators manage, remediate, and enforce user access policies to ensure effective segregation of duties using GRC integrated with Identity Management products to prevent segregation of duties control violations before they occur, and ensure user access provisioning that complies with the segregation of duties policies.

Segregation of duties ensure that no single individual has control over two or more phases of a business transaction or operation. Oracle Fusion Applications use a single segregation of duties control system, the Application Access Controls Governor (AACG).

For information on managing segregation of duties, see the Oracle Application Access Controls Governor Implementation Guide and Oracle Application Access Controls Governor User's Guide.

Security Standards: How They Are Applied

Security standards and tools used to secure Oracle Fusion Applications during implementation and when deployed deliver an integrated security approach.

Security Standards Used By Oracle Fusion Applications

The following standards and tools support security across Oracle Fusion Applications

- Role-based access control (RBAC)
- Lightweight Directory Access Protocol (LDAP)
- Java Authentication and Authorization Service (JAAS)

These standards are complied with during Oracle Fusion Applications certification.

How Security Standards and Tools Are Used

Security standards and tools in the Oracle Fusion Applications environment prohibit unauthorized access without requiring settings to be changed manually.

Role-Based Access Control

The role-based access control (RBAC) standard is applied to Oracle Fusion Applications function and data security to enforce user access based on the role of the user within the organization rather than just the user's individual identity.

- Security administration organizes access entitlement by roles to reflect business policies
- Role hierarchies and constraints express security polices
- Authorization constraints, such as segregation of duties (SOD), prevent information misuse

The effectiveness of the standard is limited by roles too broadly defined with duties and provisioned to users for whom some of those duties may not be appropriate. The Oracle Fusion Applications security reference implementation provides a full range of fine grained role definitions.

Lightweight Directory Access Protocol

LDAP provides an Oracle Fusion Applications deployment with lookup and communications services on the identity and policy stores.

Java Authentication and Authorization Service

Java Authentication and Authorization Service (JAAS) is a standard interface used for integrating with internal and third party sources for authentication and authorization, including LDAP and Single Sign On.

Oracle Platform Security Services (OPSS) provides tools and services for recording, reorganizing, and reviewing features of Oracle Fusion Applications security:

- Users across Oracle Fusion Applications
- Enterprise roles that are provisioned to users
- Application roles that each application provides to fulfill an enterprise role
- Entitlement that is granted to application roles
- Access to services, web pages, and individual widgets

Security Principles: How They Are Applied

Understanding how Oracle Fusion applies common security principles may be helpful in planning your Oracle Fusion Applications deployment.

Standard Security Principles

Oracle Fusion Applications applies the following standard security principles:

- Least privilege
- Segregation of duties
- Containment and no write down
- Transparency
- Assured revocation
- Defense in depth

Adherence to these principles enhances Oracle Fusion Applications security.

Note

Changes and custom implementations required by your enterprise may reverse the protections provided by these principles.

How Security Principles Are Applied

Oracle Fusion Applications applies security privileges using a specific implementation of features and various supporting tools.

Least Privilege

Oracle Fusion Applications roles carry only required privileges. Application roles define duties that entitle access to only the functions and data necessary for performing the defined tasks of that duty.

Segregation of Duties

Oracle Fusion Applications checks duty roles for segregation of duties policy violations measured against content and the risks defined in the Oracle Application Access Controls Governor (AACG) and against content according to best available security guidelines. User and role provisioning respects the segregation of duties policies.

Containment and No Write Down

Secured information cannot move from more to less secure stores, such as the unsecured search index, data warehouse, or a test database. Oracle Fusion Applications enforces security policies consistently across tools, access methods, and the entire information life cycle from data at rest and in transit to clones and backups.

Oracle Fusion Applications does not write sensitive information from an environment that applies restrictions to gain access to that sensitive information to one that does not. For example, Oracle Fusion Applications does not write personally identifiable information that is sensitive and private, such as national identifiers or home contact details, from Human Capital Management (HCM) to the Lightweight Directory Access Protocol (LDAP) stores. This policy extends to attachments.

Transparency

Function, data, and segregation of duties security policies are readable in plain language wherever policies are viewed or managed. Oracle Fusion Applications provides view access to implemented roles and security policies through Oracle Identity Management (OIM) and Authorization Policy Manager (APM), as well as security reference manuals and business analysis consoles.

In addition, the following optional products provide additional transparency and are certified for use with Oracle Fusion Applications:

- Oracle Database Vault
- Enterprise Manager Data Masking

Assured Revocation

Revoking one security policy revokes all implementations of that policy across all tools in production.

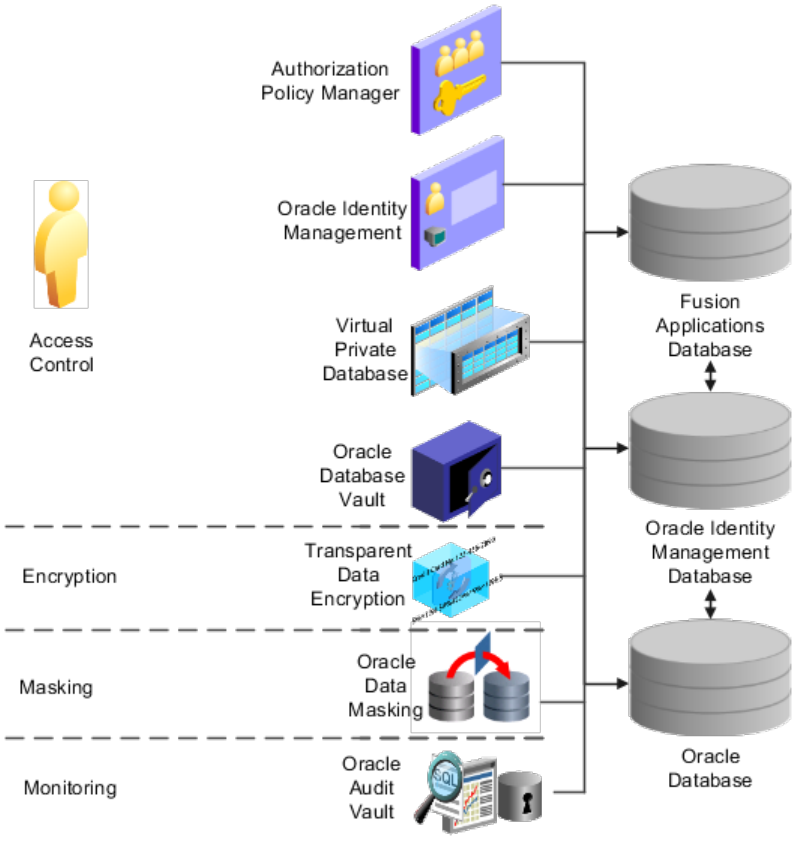
Defense In Depth

Personnel, technology, and operations are secured with multiple layers of defense across the life cycle of the information in motion, while at rest, and when accessed or used. In Oracle Fusion Applications, segregation of duties, authentication and password security, encryption, and logging and auditing are mechanisms of redundant defense that enforce protection. A comprehensive defense-in-depth approach to protecting private and sensitive data includes securing sensitive data at rest or stored in database files and their backups, as well as in transit.

The following products provide defense in depth.

Defense	Product certified for use with Oracle Fusion Applications	Installed?	Details
Monitoring	Oracle Audit Vault	Optional	Collects data and provides insight into who did what to which data when, including privileged users such as database administrators (DBA)
Access control	Oracle Database Vault	Optional	Prevents highly privileged users (DBA) from accessing application data
	Oracle Identity Management	Yes	
	Authorization Policy Manager	Yes	
	Virtual Private Database	Yes	
Encryption and Masking	Oracle Advanced Security	Optional	Protects stored, confidential data with encryption keys external to the database
	Transparent Data Encryption	Optional	
	Oracle Data Masking	Optional	Converts nonproduction data irreversibly, but optionally in formats that enable applications to function without error

The figure shows the products that provide defense in depth with access control, encryption, masking, and monitoring.



Security Products: How They Are Applied

Products used to secure implementations and deployments of Oracle Fusion Applications include function and data access management through vaulting, encryption or masking, and controls.

Security Products Used By Oracle Fusion Applications

The following integrated products support security across Oracle Fusion Applications

- Oracle Identity Management (OIM)
- Oracle Application Access Controls Governor (OAACG)
- Oracle Web Services Manager (OWSM)
- Oracle HTTP Server

Additional products are available for enhanced protections.

- Oracle Audit Vault

- Oracle Access Manager
- Oracle Role Manager
- Oracle Entitlement Server
- Oracle Virtual Directory
- Oracle Transparent Data Encryption (TDE)
- Oracle Database Vault

How Security Products Are Used

Security products in the Oracle Fusion Applications technology stack establish prohibitions to unauthorized access without requiring changes to be made in applications.

- Business intelligence
- Policy and identity stores
- Database protections
- Optional database vaulting
- Optional data encryption and masking
- Controls

Business Intelligence

Monitoring, reporting, and analysis capabilities available through the Oracle Business Intelligence Foundation Suite for Oracle Applications (OBIFA) components of Oracle Fusion Applications support adherence to or compliance with regulations. Reports of roles by product, functional privileges by role, and data security policies by role allow security professionals to modify and adapt their deployment of Oracle Fusion Applications security. Access to BI reports is also under role-based access control.

Policy and Identity Stores

Oracle Fusion Applications policy and identity stores are implemented using the Lightweight Directory Access Protocol (LDAP) store in Oracle Internet Directory to record and serve Oracle Fusion Applications security with repositories of users, roles, identities, policies, credentials, and other security elements.

Enterprise roles are implemented as LDAP Groups.

The policy store includes function security policies. Policies define security rules in XML and can be viewed and managed using Authorization Policy Manager.

Enterprise roles and role hierarchies of the reference implementation are stored in the identity store and available to the users you add to the identity store for your enterprise. The data security policies of the reference implementation are stored in the policy store. Data security policies reference duty roles to assert exactly what a job or abstract role means.

Vaulting and Database Protections

Vaults serve to protect categories of data from improper access.

- A database vault protects sensitive data from highly privileged users such as database administrators (DBA).

- An audit vault secures archives of audit data with reports and alerts that notify of access to sensitive information.
- A virtual privacy boundary on data protects personally identifiable information (PII) attribute values.

For example, Oracle Database Vault is certified for use with Oracle Fusion Applications. ODV can be used to secure sensitive data that is not PII. If Oracle Fusion Applications is deployed with ODV, the vault can protect credit card information, which reduces the risk of insider threats with separation of duty, multi-factor authorization and command rules. If Oracle Fusion Applications is deployed without ODV, Oracle Database Encryption APIs secure confidential PII attributes such as credit card and bank account numbers with controls at the column level.

Data Encryption and Masking

Encryption and masking prevents unauthorized access to sensitive data. Oracle Fusion Applications provides protections of sensitive data using encryption APIs to mask fields in production user interfaces

Oracle Fusion Applications is certified for use with the following additional products if they are included in a deployment.

- Oracle Transparent Data Encryption (TDE)
- Data Masking tools in Oracle Enterprise Manager

Encryption protects data as it is written to the file system against unauthorized access via that file system or on backups and archives. The data can be decrypted by applications when it is retrieved. Transparent Data Encryption enables encrypting data in columns independent of managing encryption keys.

Data masking prevents views of sensitive data. Data masking in Enterprise Manager overwrites sensitive data with randomly generated data in non-production instances such as for development, testing, or diagnostics. This type of masking is irreversible and the sensitive data cannot be reconstituted.

Controls

Security controls are policies, audits, and assurances. Security controlling products include the following.

- Oracle Identity Management (OIM) centrally controls user accounts and access privileges
- Oracle Authorization Policy Manager (APM) manages the security policies that control access based on roles
- Oracle Application Access Controls Governor (OAACG) provides the segregation of duties controls library
- Oracle Virtual Private Database (VPD) applies security policies at row and column levels in the database

Each of these products, except VPD, provide user interfaces for administering security controls. VPD controls are applied by running scripts against the database.

Security Processes: How They Are Applied

Processes used to secure Oracle Fusion Applications during implementation and when deployed deliver an integrated security approach.

Security Processes Used By Oracle Fusion Applications

The following processes support security across Oracle Fusion Applications

- Authentication
- Federation
- Authorization
- Provisioning and reconciliation
- Content Management
- Monitoring and diagnostics

How Security Processes Are Used

Security processes in the Oracle Fusion Applications environment prohibit unauthorized access without requiring settings to be changed manually.

Authentication

Authentication manages who is allowed into a network or application. Once in the network or application, an entitlement of privileges manages what may be done.

Authentication works in tandem with managing identities in Lightweight Directory Access Protocol (LDAP) stores or other user directories to verify that a user is who they say they are. Password security is a primary authentication mechanism. Biometrics could be another. Authentication can be further refined by levels of demilitarized zone (DMZ) or security zones. Authentication is available as an embedded or external process using Java Authentication and Authorization Service (JAAS). For example, JAAS authenticates identities in an LDAP store or through Single Sign On in the Oracle Access Manager of Oracle Identity Management.

A user signs on and establishes an authenticated session to access secured functions, which in turn provides access to data based on entitlement granted to roles that have been provisioned to the user.

Note

Oracle Fusion Applications supports anonymous sessions, weak authentication (remember me), multi-level authentication, and global session identifiers.

The authentication mechanisms used in Oracle Fusion Applications are negotiated by the secure socket layer (SSL). User sign in can be deferred to an external authenticator using Single Sign On in the Oracle Access Manager. Authentication successes and failures are recorded in audits.

Federation

Federation enables identities and their relevant roles (entitlement) to be propagated across security domains, within and among multiple organizations.

For example, enterprises implement identity federation within their portals. Acme Inc. and Beta Corp. are business partners. Acme is a national computer parts distributor, and Beta is a computer manufacturer that makes the parts that Acme resells. Beta has several inventory and production applications within its portal, and it wants the employees of Acme to access these applications, so that Acme can operate more efficiently. Using federation, Acme provides identity information that it owns, and Beta authorizes access and serves up applications that it owns. Federation manages the credentials, profiles, and sign ins of each Acme employee that accesses Beta's applications. If an Acme employee quits or is fired and Beta is not told, that ex-employee is automatically locked out of Betas systems as soon as the user leaves Acme Inc.

Authorization

Authorization is the permission for an entity to perform some action against some resource. For example, a user's enterprise role membership authorizes access to all Oracle Fusion Applications resources needed to enable the user to fulfill the duties described by that job or abstract role. OPSS controls the authorization processes on functions and Oracle Fusion Data Security, as well as in some cases application code, control the authorization processes on data.

Segregation of duties is a type of authorization constraint that defines violations that could result in misuse of information.

Provisioning and Reconciliation

Security related provisioning involves provisioning roles and identities or people.

Human approvals secure a task using both grants and roles. Administrators and implementation consultants apply the RBAC standard in Oracle Fusion Applications to the requirements of their enterprise using provisioning tools.

Accounts are created as identities or people in the Lightweight Directory Access Protocol (LDAP) store. Roles are provisioned by making the identity a member of a group that is the requested role. LDAP records and serves Oracle Fusion Applications security with identities, policies, and credentials.

Oracle Fusion Applications notifies the IT security manager of all account requests, role provisioning requests, and grants to ensure role administration is always documented, authorized and auditable. Accounts are created as identities in the LDAP store.

Oracle Fusion Applications use the following tools to handle account and role provisioning with the stores, as well as Human Resources (HR) and Oracle Fusion Trading Community Model identity provisioning with the Oracle Fusion Applications schema.

- Oracle Fusion Human Capital Management (HCM)
- Oracle Identity Management (OIM)

Provisioning infrastructure and policies include provisioning services, temporary storage of registration data, approval and approval routing, notifications, business logic, and eligibility. Users are provisioned using the LDAP deployed for use by Oracle Fusion Applications.

Granting or revoking object entitlement to a particular user or group of users on an object instance or set of instances extends the base Oracle Fusion Applications

security reference implementation without requiring customization of the applications that access the data.

Changes to identity information are reconciled to OIM (LDAP) and thereby reconciled to users. Changes to users are not reconciled to identity information in HR.

Content Management

Oracle Fusion Applications integrates with Oracle WebCenter Content using LDAP, single sign on, and Web Services to handle attachments. By default an Oracle Fusion Applications deployment grants no access to documents through content management user interfaces. All access is through Oracle Fusion Applications.

Oracle Fusion applications apply security to files in Oracle WebCenter Content by calling a file authorization Web Service to determine whether the current user has been granted access to a file. When a user tries to access a file, Oracle Fusion applications determine whether the user is permitted access and grants access for the duration of the session.

Attached documents are only accessible through Oracle Fusion Applications user interfaces, not through content management user interfaces. Attached documents that contain sensitive information are placed in document categories that require authorization when content is accessed from within Oracle Fusion Applications. Function security rules apply to content management. Access to attachments is determined by access to the owning entity, such as a table, purchase order, agreement, or supplier account, but also to the category.

For example, a role that has access to the purchase order, such as a buyer, can view attachments in the category Note to Buyer and can create, update, and delete attachments in the category Note to Receiver. The receiver of the purchase order and receipts entity can view attachments in the category Note to Buyer and Special Handling Instructions.

All workers typically have access sufficient for viewing all other workers in a public directory, but workers should not have access to any attachments for the person. Line managers have access to workers that they manage and have access to documents such as performance review notes or anything they choose to upload, but line managers do not have access to things like tax documents or visa documents. HR specialists have access to all people for whom they are responsible and can see everything that the line manager sees, as well as visa documents, but not tax documents. Payroll specialists have access to all people for whom they are responsible and can view the tax documents. Security of person documents is implemented using Document Type security profiles.

You associate attachment categories with an entity using the Manage Attachments Categories task.

Monitoring and Diagnostics

Oracle Fusion Applications security works at runtime to prevent and detect embezzlement, such as fraud, and other acts of personal gain at the expense of an enterprise. Tools and tasks that are relevant to detection include analyzing risks carried in segregation of duties violations.

System configuration is relevant to runtime processes. Administrators determine and modify system configuration based on enterprise security requirements

and the particulars of their Oracle Fusion Applications deployment using diagnostics.

Secured Oracle Fusion Applications Deployments: Points To Consider

Considerations in deploying secure Oracle Fusion applications include the following.

- Baseline standalone deployment infrastructure
- Integrations with other applications
- Extended deployment with secured Web services
- Secured audits

Oracle Fusion Applications security is designed to control exchanges with third party or non-Fusion deployments.

Standalone Deployment

Oracle Fusion Applications are designed to be deployed as a complete applications platform.

In the absence of integrations with legacy applications or external Web services that allow data to be loaded into Oracle Fusion applications database tables, the design and reference implementation provide standalone security.

Extending a standalone deployment of Oracle Fusion Applications involves adding new entities to the Online Transaction Processing (OLTP) database table or even configuring new attributes through flexfields. Extending Fusion Applications does not include making changes to the behavior of an application unless that change involves adding new data attributes to an existing entity object and adding any new entity objects to an application.

Where Oracle Fusion Applications need to be extended, you may additionally need to install Oracle JDeveloper.

Application Identities

Calling applications use application identities (APPID) to enable the flow of transaction control as it moves across trust boundaries. For example, a user in the Distributed Order Orchestration product may release an order for shipping. The code that runs the Pick Notes is in a different policy store than the code that releases the product for shipment. When the pick note printing program is invoked it is the Oracle Fusion Distributed Order Orchestration Application Development Framework (ADF) that is invoking the program and not the end user.

Oracle Fusion Applications stores application IDs just like individuals, but in a separate branch of the identity store directory.

Before deployment, review the Lightweight Directory Access Protocol (LDAP) identity store to verify the existence of the APPIDs.

Warning

Do not change or remove application identities or their permissions.

The following application identities are predefined.

Application Identity Code	Application Identity Name
FUSION_APPS_ATK_UMS_APPID	Application Toolkit User Messaging Service Application Identity
FUSION_APPS_AMX_APPID	Approval Management Service Application Identity
FUSION_APPS_APM_RGX_APPID	Data Role Template Application Identity
FUSION_APPS_ECSF_SES_ADMIN_APPID	Oracle Fusion Search Administrator Application Identity (CRM)
FUSION_APPS_OBIA_BIEE_APPID	Business Intelligence Applications Extract Transform and Load Application Identity
FUSION_APPS_OIM_SPML_APPID	Oracle Identity Manager Application Identity
FUSION_APPS_SEARCH_APPID	Oracle Fusion Search Application Identity
FUSION_APPS_CRM_ADF_APPID	Applications Development Framework Application Identity (CRM)
FUSION_APPS_CRM_ADF_BI_APPID	Applications Development Framework Business Intelligence Application Identity (CRM)
FUSION_APPS_CRM_ADF_SOAP_APPID	Applications Development Framework SOAP Application Identity (CRM)
FUSION_APPS_CRM_DIAGNOSTICS_APPID	Applications Diagnostic Framework Application Identity (CRM)
FUSION_APPS_CRM_ECSF_SEARCH_APPID	Enterprise Search and Crawl Framework Application Identity (CRM)
FUSION_APPS_CRM_EM_APPID	Oracle Enterprise Manager Application Identity (CRM)
FUSION_APPS_CRM_ESD_APPID	Email Sending Daemon Application Identity (CRM)
FUSION_APPS_CRM_ESS_APPID	Enterprise Scheduler Job Application Identity (CRM)
FUSION_APPS_CRM_ESS_REPORT_APPID	Enterprise Scheduler Reporting Application Identity (CRM)
FUSION_APPS_CRM_ODI_ESS_APPID	Oracle Data Integrator Application Identity (CRM)
FUSION_APPS_CRM_ODI_SUPERVISOR_APPID	Oracle Data Integrator Supervisor Application Identity (CRM)
FUSION_APPS_CRM_SELFSERVICE_ADF_APPID	Applications Development Framework Self Service Application Identity (CRM)
FUSION_APPS_CRM_SES_CRAWL_APPID	Oracle Fusion Search Application Identity (CRM)
FUSION_APPS_CRM_SOA_APPID	Web Services Application Identity (CRM)
FUSION_APPS_FIN_ADF_APPID	Applications Development Framework Application Identity (Financials)
FUSION_APPS_FIN_EMPNATID_APPID	Employee National Identifiers Application Identity
FUSION_APPS_FIN_ESS_EMPMTCH_APPID	Employee Matching Application Identity (Financials)
FUSION_APPS_FIN_IPM_APPID	Document Management Integration Application Identity (Financials)
FUSION_APPS_FIN_SOA_APPID	Web Services Application Identity (Financials)

FUSION_APPS_FSCM_DIAGNOSTICS_APPID	Applications Diagnostic Framework Application Identity (FSCM)
FUSION_APPS_FSCM_ECSF_SEARCH_APPID	Enterprise Search and Crawl Framework Application Identity (FSCM)
FUSION_APPS_FSCM_EM_APPID	Oracle Enterprise Manager Application Identity (FSCM)
FUSION_APPS_FSCM_SES_CRAWL_APPID	Oracle Fusion Search Application Identity (FSCM)
FUSION_APPS_HCM_DIAGNOSTICS_APPID	Applications Diagnostic Framework Application Identity (HCM)
FUSION_APPS_HCM_ECSF_SEARCH_APPID	Enterprise Search and Crawl Framework Application Identity (HCM)
FUSION_APPS_HCM_EM_APPID	Oracle Enterprise Manager Application Identity (HCM)
FUSION_APPS_HCM_ESS_APPID	Enterprise Scheduler Job Application Identity (HCM)
FUSION_APPS_HCM_ESS_LOADER_APPID	Batch Loader Enterprise Scheduler Job Application Identity (HCM)
FUSION_APPS_HCM_ODI_ESS_APPID	Oracle Data Integrator Application Identity (HCM)
FUSION_APPS_HCM_ODI_SUPERVISOR_APPID	Oracle Data Integrator Supervisor Application Identity (HCM)
FUSION_APPS_HCM_SES_CRAWL_APPID	Oracle Fusion Search Application Identity (HCM)
FUSION_APPS_HCM_SOA_APPID	Web Services Application Identity (HCM)
FUSION_APPS_HCM_SOA_SPML_APPID	Service Provisioning Markup Language Interface Application Identity (HCM)
FUSION_APPS_WCFORUM_ADMIN_APPID	Web Center Forum Application Identity
FUSION_APPS_WEBCENTER_CRAWL_APPID	Oracle WebCenter Crawl Application Identity
FUSION_APPS_WSM_APPID	Web Services Manager Application Identity
FUSION_APPS_PRC_ADF_APPID	Applications Development Framework Application Identity (Procurement)
FUSION_APPS_PRC_ESS_APPID	Enterprise Scheduler Job Application Identity (Procurement)
FUSION_APPS_PRC_SOA_APPID	Web Services Application Identity (Procurement)
FUSION_APPS_PRJ_ADF_APPID	Applications Development Framework Application Identity (Projects)
FUSION_APPS_PRJ_ESS_APPID	Enterprise Scheduler Job Application Identity (Projects)
FUSION_APPS_PRJ_SOA_APPID	Web Services Application Identity (Projects)
FUSION_APPS_SCM_ADF_APPID	Applications Development Framework Application Identity (SCM)
FUSION_APPS_SCM_ESS_APPID	Enterprise Scheduler Job Application Identity (SCM)
FUSION_APPS_SCM_SOA_APPID	Web Services Application Identity (SCM)
FUSION_APPS_SETUP_ESS_APPID	Enterprise Scheduler Job Application Identity (Setup)

Application Identity Password Reset And Password Policy Management

As a security guideline, reset application identity passwords periodically during scheduled downtimes. For example, when moving application identities from

one environment to another as part of moving an identity store, you must reset the passwords so they are unique to an environment. Reset the APPID passwords using the following command.

Restriction

This command can be run only after the Oracle WebLogic Server installation for the Oracle Fusion Applications domain is set up.

Run the following command to get the list of all the entries for which the passwords need to be set:

```
Ldapsearch -h ldapHost -p ldapPort -D binddn -w password -b
 'cn=appidusers,cn=users,namigncontext' -s sub 'objectclass=orclAppiduser'
 cn >& reset.txt
ORACLE_HOME/idmtools/bin/appidtool.sh pwdreset -ldapHost
 tuvwxy0123.us.example.com -ldapPort 3060 -ldapUser cn=orcladmin -wlsHost
 tuvwxy0123.us.example.com -wlsPort 7001 -wlsUser weblogic -file reset.txt
 -userBase cn=users,namingcontext
```

Variable	Refers to the value for:
`ldapHost`	Identity store host
`ldapPort`	Identity store port
`ldapUser`	User name for connecting to the identity store. This user should have the entitlement necessary to reset the APPID passwords.
`wlsHost`	Administration Server on the Oracle Fusion Applications domain
`wlsPort`	Administration Server port on the Oracle Fusion Applications domain
`reset.txt`	The file that contains the list of application identities for which the passwords need to be set
`userBase`	The user base under which the application identities exist

Integrations With Other Applications

Integrating Oracle Fusion Applications with other applications, including other Oracle Applications product lines, require decisions in the following areas.

- Central Lightweight Directory Access Protocol (LDAP) repository
- Data migration
- Coordination of Oracle Fusion Applications roles to legacy function security control

For example, coordinate Oracle Fusion Applications roles to responsibilities and menu paths in Oracle eBusiness Suite (EBS) for integration between EBS and Oracle Fusion Applications.

Note

Duty roles are not propagated or synchronized across Oracle Fusion Middleware, where they are considered to be application roles.

When implementing a system-to-system integration with an external system, you may need to identify that system in the identity store in order to grant that system permissions.

Extending Oracle Fusion Applications With a Secured Web Service

If you extend your Oracle Fusion Applications deployment with a Web service that allows external users to load data into database interface tables, consider the following requirements.

- Implement authentication
- Implement authorization checks; though not required, their absence allows sharing of identities, which removes your ability to audit the access.
- Create a regular identity for the external user with the appropriate function and data security access.

For example, create a new duty role with the desired data access entitlement, privilege to submit an Oracle Enterprise Scheduler Service job, and permission to access the Web Service.

For information about securing Web services and task flows when extending applications, see the Oracle Fusion Applications Security Hardening Guide.

Tuning and Maintaining Deployments

Tuning and maintaining Oracle Fusion Applications security includes auditing, managing changes, and handling leaks, threats, and inappropriate access.

Tasks that consume Web services exposed to Enterprise Manager (EM) require specific duty roles to be provisioned to the users performing those tasks. For example, the user connecting to the Web service that EM uses to collect metrics must be provisioned with the FUN_BU_ADMIN_DUTY role.

Avoid provisioning users who are under audit with roles that are entitled to manage audits and audit results. Avoid provisioning users who are under audit with roles that entitle access to protected data the users are otherwise not permitted to access.

Tip

Avoid entitling users who configure audits from being the same users who performed the activities under audit.

For information about elevating access privileges for a scheduled job, see the Oracle Fusion Applications Developer's Guide for Oracle Enterprise Scheduler.

4

Role-Based Access Control

Role-Based Access Control: Explained

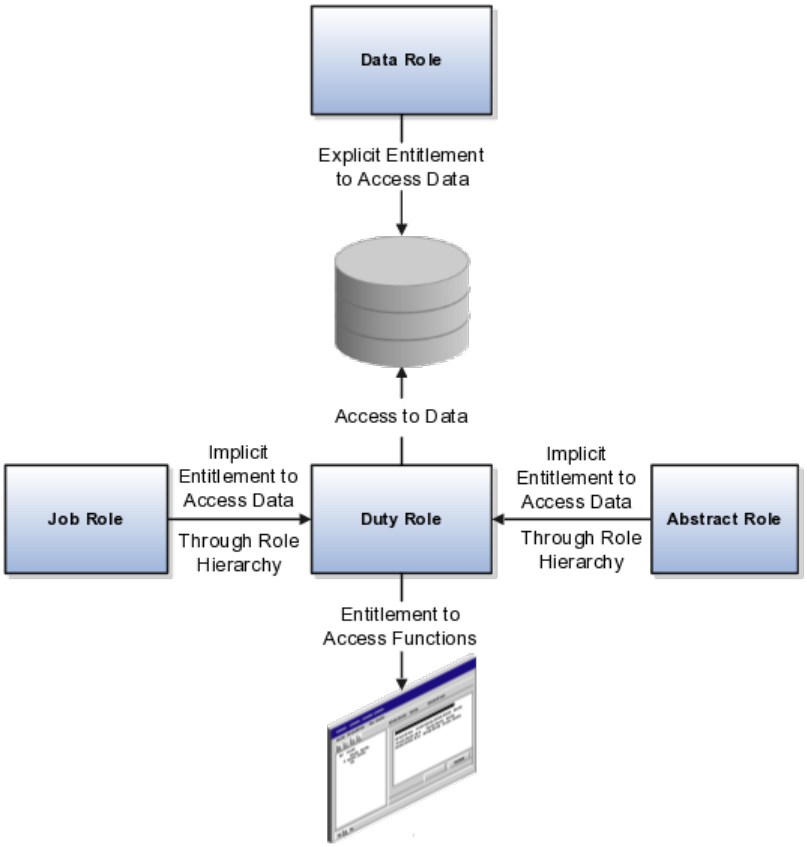
Role-based access control (RBAC) normalizes access to functions and data through user roles rather than only users. User access is based on the definition of the roles provisioned to the user.

RBAC secures access in a "Who can do what on which functions or sets of data under what conditions" approach. The "who" is the user.

The "what" are the abstract operations or entitlement to actions applied to resources. For example, view and edit are actions, and task flows or rows in data tables are resources.

Entitlement secures access rights to application functions and data. Function access entitlement is granted explicitly to duty roles. This implicitly grants the function access to the job and abstract roles that inherit the duty roles. Data access entitlement is granted implicitly to abstract and job roles through data security policies on their inherited duty roles. Data access entitlement is granted explicitly to a data role through a data security policy applied directly to the inherited job or abstract role.

The following figure shows the implicit and explicit access entitlements of the role types. The Accounts Payable Manager: USA grants explicit access to Payables Invoices in the USA data dimension. The Sales Party Review Duty role grants access to Sales Party data. A Marketing Analyst includes the Sales Party Review Duty role in its hierarchy, which provides the Marketing Analyst with implicit access to the Sales Party data. A data security policy states that a Marketing Analyst can view sales party where user is in the management chain of a resource who is on the sales account team.



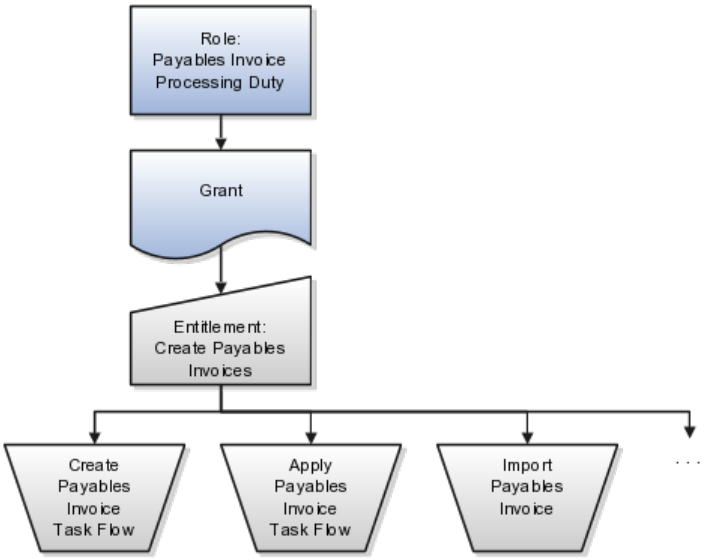
In the security reference implementation, an example of a data role generated by a predefined data role template in an enterprise with a business unit named US is an Accounts Payable Manager - US role that inherits the Accounts Payable Manager job role. The data role grants explicit access to Payables Invoices in the US data dimension.

An example of a duty role is the Sales Party Review Duty role, which grants access to Sales Party data. Another example of a job role is the Marketing Analyst role, which includes the Sales Party Review Duty role in its hierarchy. The Sales Party Review Duty role provides the Marketing Analyst with implicit access to the Sales Party data. A data security policy states that a Marketing Analyst can view sales party information where user is in the management chain of a resource who is on the sales account team.

An example of an abstract role is the Employee role, which inherits duty roles that entitle access to functions and data belonging to tasks performed by all employees, such as entering requisitions.

As a security guideline, grants are made to duty roles, and duty roles are given as children to job or abstract roles. Grants are also made to data roles.

The figure shows how grants include sets of entitlement that capture the access and action rights of a duty role.



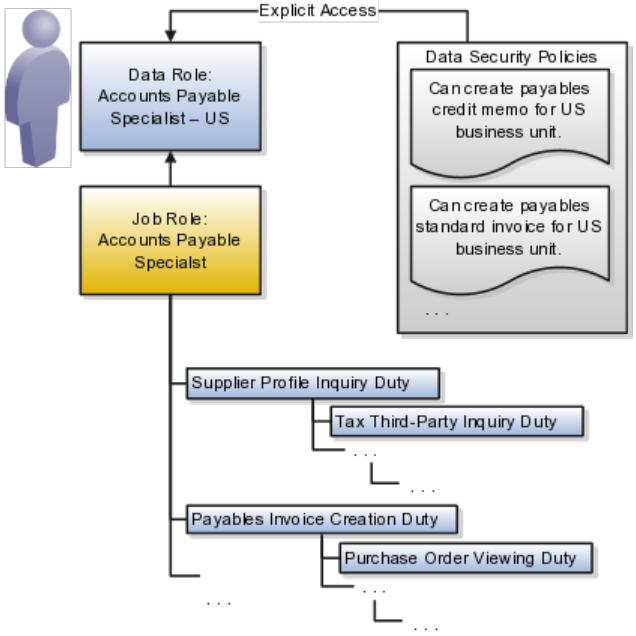
Explicit Access

An explicit entitlement names the specific function or data that the holder of the entitlement is authorized to access.

Only duty roles hold explicit entitlement to functions. An entitlement to a function allows one or more actions, such as update, create, and view applied to a resource, such as a task flow.

Data roles hold explicit entitlement to data. Data roles are entitled access to functions through inherited role hierarchies. Data roles are entitled access to data through conditional grants on each object. In most cases, the data you secure in your enterprise is secured with data roles.

In the following example, the user provisioned with a data role carries explicit access specifically to the US business unit dimension of data relevant for an accounts payables specialist.



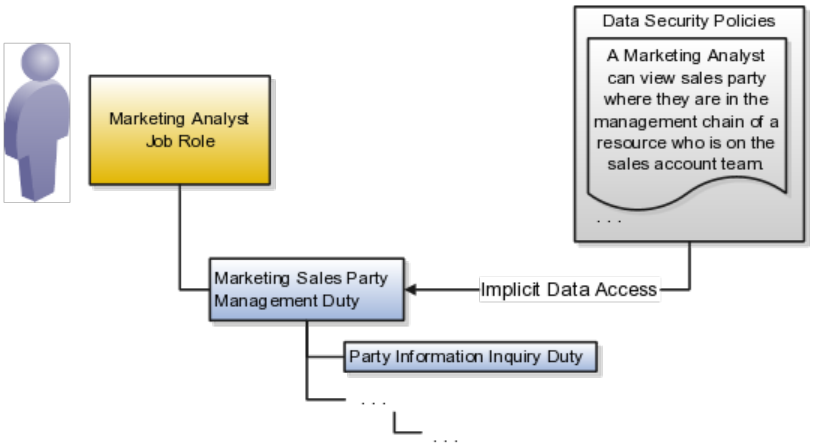
Implicit Access

An implicit entitlement names roles to which explicit entitlement is granted through a role hierarchy.

Abstract, job, and data roles have implicit access to functions through duty roles that they inherit. Abstract, job, and duty roles have implicit access to data through data security policies. Data is also secured implicitly with the underlying data model of the product family records, which contain all the information required to enable Oracle Fusion data security. For example: A person assigned to a task is recorded in a project table, and the data in the record drives the security on that data. No provisioning is required to enable project team access. Typically a business event is raised that enables a human workflow approval of the action.

Implicit data access is easier to manage and maintain than explicit data access, but not available when requirements can only be met using explicit data access.

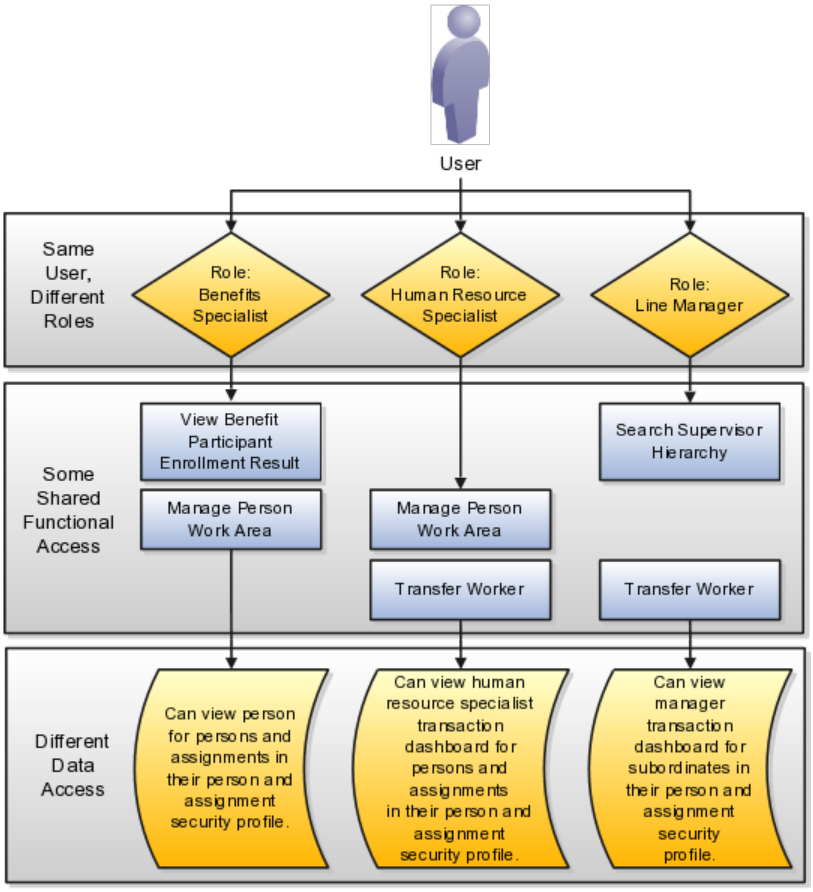
In the following example, the user provisioned with a job role carries implicit access through a role hierarchy with duty roles that participate in data security policies defining access to data required for performing the duties of that job.



User With Multiple Roles

A user who fills multiple roles in the organization should be provisioned with multiple roles for security reasons so changes in responsibility can be quickly applied. The user's functional and data access is the union of grants provided by the provisioned roles.

For example, a user can be provisioned with the Benefits Specialist, Human Resources Specialist, and Line Manager roles. These roles grant different, though partially overlapping, functional access, and differing data access.



One role gives the user access to one subset of functions and data, while another role gives access to another subset. For example, in Human Capital Management (HCM) the human resources (HR), payroll, and benefits roles carry entitlements to access different parts of a process. For example, a human resources specialist, a line manager, and an employee can perform the following tasks.

- Human resource specialists function against the set of people that they administer.
- Line managers function against the people who report to them.
- Self-service employees function against themselves.

Role Types : How They Fit Together

Oracle Fusion Applications security provides abstract, job, data, and duty roles that work together to control access to functions and data.

Note

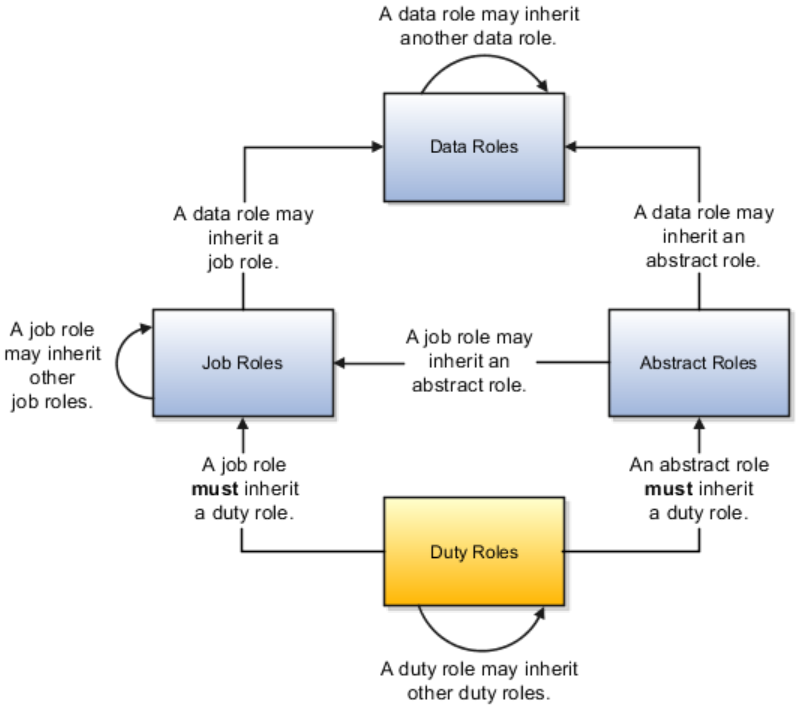
Abstract, job, and data roles are enterprise roles in Oracle Fusion Applications. Oracle Fusion Middleware products such as Oracle Identity Manager (OIM)

and Authorization Policy Manager (APM) refer to enterprise roles as external roles. Duty roles are implemented as application roles in APM and scoped to individual Oracle Fusion Applications.

Abstract roles identify a general association to the enterprise or organization, such as employee or line manager. Job roles reflect job titles and describe positions of responsibility, such as Payables manager or buyer. Data roles identify entitlement to access specific data. Duty roles group tasks that must be performed within an abstract or job role.

Oracle Fusion Applications record abstract, job, and data roles as enterprise roles shared across multiple applications and instances of applications. Duty roles function at the application level and are a grouping of tasks to be done within an abstract or job role.

Abstract and job roles must inherit duty roles. Job roles may inherit abstract roles and other job roles. Data roles may inherit abstract, job, and other data roles. Duty roles may inherit other duty roles. The figure shows these inheritance relationships among role types.



For example, a data role defined as Accounts Payable Manager - US inherits the job role Accounts Payable Manager. The job role Accounts Payable Manager inherits the duty role Approving Payable Invoices Duty and the abstract role Line Manager.

Note

In the reference implementation, the Payables Manager does not inherit the Line Manager role. This example represents an enterprise specific modification to the reference implementation.

Provisioning

You provision enterprise roles to users. Enterprise roles inherit a hierarchy of roles. Application roles are not directly provisioned to users. When you initiate a provisioning event in Oracle Fusion Applications you invoke Oracle Identity Management.

Where data roles are available, they should be provisioned rather than provisioning the job roles they inherit.

Role Hierarchy

Roles form hierarchical groups. Entitlement can be inherited from one or more child roles in a role hierarchy. You manage role hierarchies in APM.

Adding roles to a hierarchy may introduce segregation of duties policy violations by authorizing a provisioned user with access that can lead to deliberate or inadvertent fraud.

5

Function Security

Function Security: Explained

Function security consists of privileges unconditionally granted to a role and used to control access to a page or a specific widget or functionality within a page, including services, screens, and flows, and typically used in control of the main menu. Function security involves granting a user, by means of the user's membership in a role, the ability to perform operations in pages or task flows such as view or manage.

Function Security Policies

A function security policy consists of privileges assigned to duty roles and those duty roles assigned to a job or abstract role. Function security policies are defined in the Authorization Policy Manager (APM).

Implementation

Function security is implemented using JAAS (Java Authentication and Authorization Services) permissions representing an Application Development Framework (ADF) artifact. These permissions are stored in the Oracle Platform Security Services (OPSS) policy store and are checked by Application Development Framework (ADF) at runtime.

When a user accesses the functions of a task flow, the OPSS policy store determines the access entitlement that applies to that user through the roles provisioned to the user.

Securing Functions: Points to Consider

The functions that a user can access via roles are interface elements, such as the pages or widgets of a task flow.

Functions are organized separately from menu navigation and access to functions is granted to users via roles. Policies comprised of grants with access entitlement to components are stored in the policy store, and application roles within role hierarchies are defined with access rights through policies. The access

entitlement to a component consists of allowable actions, or privilege, on the component.

Users of Oracle Fusion Applications must be able to access the functions necessary for performing their jobs and be excluded from functions that are irrelevant or improper to their roles in the enterprise. This may require changes to the roles available for provisioning.

For the broadest possible access to the functionality in Oracle Fusion Applications, the role to which broad entitlement is granted would be a role high in the role hierarchy, such as worker. Such broad entitlement should not include access rights to any functions that violate the security policies of the enterprise, but allow performance of all duties associated with the role.

Job Role Changes

A job role is constructed by identifying each of the duty roles and abstract roles it inherits. In Oracle Identity Manager (OIM) and Applications Authorization Policy Manager (APM), job roles are external roles and duty roles are application roles.

No function security privileges can be assigned directly to a job role. Job roles may inherit other job roles, abstract and duty roles. Data security policies using either job or duty roles may reference data entitlement. The reference within the data security policy to a duty role is a security guideline because it allows more flexibility in asserting exactly what any given job means.

Most job role changes are created by implementing role hierarchies of the predefined Oracle Fusion Applications roles in ways that fulfill the needs of your enterprise.

Create a new job role by creating a new group in the Lightweight Directory Access Protocol (LDAP) Store and mapping the duties to the group in the role hierarchy.

Duty Role Changes

Duty roles are one of the building blocks of Oracle Fusion Applications security.

Duty roles may carry both function and data security grants. As a security guideline, make duty roles self-contained and pluggable into any existing or new job or abstract role to avoid introducing definition conflicts in the owning application.

New duty roles may be required with extensions for Oracle Fusion Applications. All predefined Oracle Fusion Applications functions that need to be secured correspond to a duty role. A duty role should carry no segregation of duties risk within it.

Data Role Changes

A data role carries the function security entitlement inherited from the role hierarchies and data security entitlement conditionally granted on each object and condition.

Implementation consultants typically define data roles required by the data requirements of the enterprise. Commonly data roles limit access for control and performance reasons within tools, applications, or areas of a deployment such as department or cost centers.

Role Incompatibilities

Role incompatibility can occur in function control, as well as in segregation of duties.

FAQs for Role Based Access Control

What's the difference between an enterprise role and an application role?

Enterprise roles are the abstract, job, and data roles shared across all applications. Enterprise roles and role memberships are stored in the Lightweight Directory Access Protocol (LDAP) identity store. Oracle Identity Manager (OIM) and Applications Authorization Policy Manager (APM) refer to enterprise roles as external roles.

An application role is supplied by a single application or pillar of applications. Application roles are stored in the policy store.

Users acquire application function and data access by being granted membership to an enterprise role.

In the security reference implementation, an application role corresponds to a duty role. Users acquire duty role privileges by being provisioned with the parent job or abstract roles of the duty role. Security policies in the policy stores (LDAP and Oracle Fusion Data Security) define which functions and data the duty role is authorized to access.

Both enterprise and application roles participate in security policies.

6

Data Security

Data Security: Explained

By default, users are denied access to all data.

Data security makes data available to users by the following means.

- Policies that define grants available through provisioned roles
- Policies defined in application code

You secure data by provisioning roles that provide the necessary access. Enterprise roles provide access to data through data security policies defined for the inherited application roles.

When setting up the enterprise with structures such as business units, data roles are automatically generated that inherit job roles based on data role templates. Data roles also can be generated based on HCM security profiles. Data role templates and HCM security profiles enable defining the instance sets specified in data security policies.

When you provision a job role to a user, the job role implicitly limits data access based on the data security policies of the inherited duty roles. When you provision a data role to a user, the data role explicitly limits the data access of the inherited job role to a dimension of data.

Data security consists of privileges conditionally granted to a role and used to control access to the data. A privilege is a single, real world action on a single business object. A data security policy is a grant of a set of privileges to a principal on an object or attribute group for a given condition. A grant authorizes a role, the grantee, to actions on a set of database resources. A database resource is an object, object instance, or object instance set. An entitlement is one or more allowable actions applied to a set of database resources.

Data is secured by the following means.

Data security feature	Does what?
Data security policy	Grants access to roles by means of entitlement
Role	Applies data security policies with conditions to users through role provisioning.

Data role template	Defines the data roles generated based on enterprise setup of data dimensions such as business unit.
HCM security profile	Defines data security conditions on instances of object types such as person records, positions, and document types without requiring users to enter SQL code
Masking	Hides private data on non-production database instances
Encryption	Scrambles data to prevent users without decryption authorization from reading secured data

The sets of data that a user can access via roles are defined in Oracle Fusion Data Security. Oracle Fusion Data Security integrates with Oracle Platform Security Services (OPSS) to entitle users or roles (which are stored externally) with access to data. Users are granted access through the entitlement assigned to the roles or role hierarchy with which the user is provisioned. Conditions are WHERE clauses that specify access within a particular dimension, such as by business unit to which the user is authorized.

Data Security Policies

Data security policies articulate the security requirement "Who can do What on Which set of data," where 'Which set of data' is an entire object or an object instance or object instance set and 'What' is the object entitlement.

For example, accounts payable managers can view AP disbursements for their business unit.

Who	can do	what	on which set of data
Accounts payable managers	view	AP disbursements	for their business unit

A data security policy is a statement in a natural language, such as English, that typically defines the grant by which a role secures business objects. The grant records the following.

- Table or view
- Entitlement (actions expressed by privileges)
- Instance set (data identified by the condition)

For example, disbursement is a business object that an accounts payable manager can manage by payment function for any employee expenses in the payment process.

Note

Some data security policies are not defined as grants but directly in applications code. The security reference manuals for Oracle Fusion Applications offerings differentiate between data security policies that define a grant and data security policies defined in Oracle Fusion applications code.

A business object participating in a data security policy is the database resource of the policy.

Data security policies that use job or duty roles refer to data security entitlement.

For example, the data security policy for the Accounts Payable Manager job role refers to the view action on AP disbursements as the data security entitlement.

Important

The duty roles inherited by the job role can be moved and job roles reassembled without having to modify the data security.

As a security guideline, data security policies based on user session context should entitle a duty role. This keeps both function and data security policies at the duty role level, thus reducing errors.

For example, a Sales Party Management Duty can update Sales Party where the provisioned user is a member of the territory associated with the sales account. Or the Sales Party Management Duty can update Sales Party where the provisioned user is in the management chain of a resource who is on the sales account team with edit access. Or the Participant Interaction Management Duty can view an Interaction where the provisioned user is a participant of the Interaction.

For example, the Disbursement Process Management Duty role includes entitlement to build documents payable into payments. The Accounts Payable Manager job role inherits the Disbursement Process Management Duty role. Data security policies for the Disbursement Process Management Duty role authorize access to data associated with business objects such as AP disbursements within a business unit. As a result, the user provisioned with the Accounts Payable Manager job role is authorized to view AP disbursements within their business unit.

A data security policy identifies the entitlement (the actions that can be made on logical business objects or dashboards), the roles that can perform those actions, and the conditions that limit access. Conditions are readable WHERE clauses. The WHERE clause is defined in the data as an instance set and this is then referenced on a grant that also records the table name and required entitlement.

Data Roles

Data roles are implemented as job roles for a defined set of data.

A data role defines a dimension of data within which a job is performed. The data role inherits the job role that describes the job. For example, a data role entitles a user to perform a job in a business unit.

The data role inherits abstract or job roles and is granted data security privileges. Data roles carry the function security privileges inherited from job roles and also the data security privilege granted on database objects and table rows.

For example, an accounts payables specialist in the US Business Unit may be assigned the data role Accounts Payables Specialist - US Business Unit. This

data role inherits the job role Accounts Payables Specialist and grants access to transactions in the US Business Unit.

A data role may be granted entitlement over a set people.

For example, a Benefits Administrator A-E is allowed to administer benefits for all people that have a surname that begins with A-E.

Data roles are created using data role templates. You create and maintain data roles in the Authorization Policy Manager (APM). Use the Manage Data Roles and Security Profiles task to create and maintain HCM data roles in Oracle Fusion HCM.

HCM Security Profiles

HCM security profiles are used to secure HCM data, such as people and departments. You use HCM security profiles to generate grants for an enterprise role. The resulting data role with its role hierarchy and grants operates in the same way as any other data role.

For example, an HCM security profile identifies all employees in the Finance division.

Oracle Fusion Payroll uses HCM security profiles to secure project organizations. Applications outside of HCM can use the HCM Data Roles UI pages to give their roles access to HR people.

Masking and Encryption

Oracle Fusion Applications uses masking to protect sensitive data from view by unauthorized users. Encryption APIs mask sensitive fields in applications user interfaces. Additionally, Oracle Data Masking is available for masking data in non-production instances and Oracle Transparent Data Encryption is available for protecting data in transit or in backups independent of managing encryption keys.

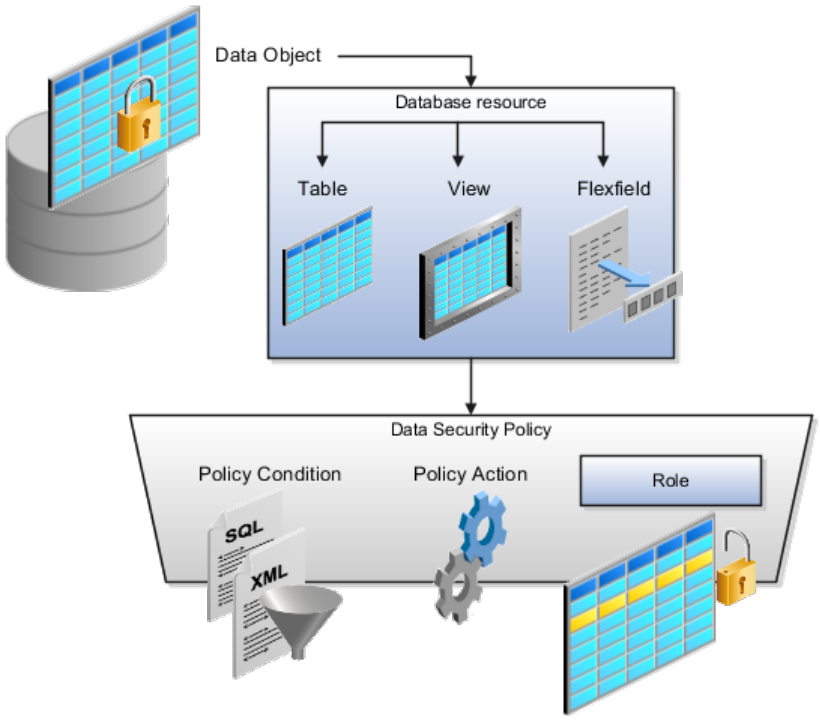
Database Resources and Data Security Policies: How They Work Together

A data security policy applies a condition and allowable actions to a database resource for a role. When that role is provisioned to a user, the user has access to data defined by the policy. In the case of the predefined security reference implementation, this role is always a duty role. Data roles generated to inherit the job role based on data role templates limit access to database resources in a particular dimension, such as the US business unit.

The database resource defines and instance of a data object. The data object is a table, view, or flexfield.

The following figure shows the database resource definition as the means by which a data security policy secures a data object. The database resource names

the data object. The data security policy grants to a role access to that database resource based on the policy's action and condition.



Database Resources

A database resource specifies access to a table, view, or flexfield that is secured by a data security policy.

- Name providing a means of identifying the database resource
- Data object to which the database resource points

Data Security Policies

Data security policies consist of actions and conditions for accessing all, some, or a single row of a database resource.

- Condition identifying the instance set of values in the data object
- Action specifying the type of access allowed on the available values

---

Note

If the data security policy needs to be less restrictive than any available database resource for a data object, define a new data security policy.

Actions

Actions correspond to privileges that entitle kinds of access to objects, such as view, edit, or delete. The actions allowed by a data security policy include all or a subset of the actions that exist for the database resource.

Conditions

A condition is either a SQL predicate or an XML filter. A condition expresses the values in the data object by a search operator or a relationship in a tree hierarchy. A SQL predicate, unlike an XML filter, is entered in a text field in the data security user interface pages and supports more complex filtering than an XML filter, such as nesting of conditions or sub queries. An XML filter, unlike a SQL predicate, is assembled from choices in the UI pages as an AND statement.

Tip

An XML filter can be effective in downstream processes such as business intelligence metrics. A SQL predicate cannot be used in downstream metrics.

Securing Data Access: Points to Consider

Oracle Fusion Applications supports securing data through role-based access control (RBAC) by the following methods.

Method of securing data	Reason	Example
Data roles apply explicit data security policies on job and abstract roles	Appropriate for job and abstract roles that should only access a subset of data, as defined by the data role template that generates the data role or by HCM security profiles.	Accounts Payable Manager - US data role to provide an accounts payable manager in the US business unit with access to invoices in the US business unit.
Data security policies	Define data access for application roles and provide inheriting job and abstract roles with implicit data security	Projects

If a user has access to the same function through different roles that access different data sets, then the user has access to a union of those data sets.

When a runtime session is created, Oracle Platform Security Services (OPSS) propagates only the necessary user to role mapping based on Oracle Fusion Data Security grants. A grant can specify entitlement to the following.

- Specific rows of data (data object) identified by primary key
- Groups of data (instance set) based on a predicate that names a particular parameter
- Data objects or instance sets based on runtime user session variables

Data is either identified by the primary key value of the row in the table where the data is stored. Or data is identified by a rule (SQL predicate) applied to the WHERE clause of a query against the table where the data is stored.

Grants

Oracle Fusion Data Security can be used to restrict the following.

- Rows that are returned by a given query based on the intended business operation
- Actions that are available for a given row

Grants control which data a user can access.

Note

Attribute level security using grants requires a data security policy to secure the attribute and the entitlement check enforces that policy.

A grant logically joins a user or role and an entitlement with a static or parameterized object instance set. For example, `REGION='WEST'` is a static object instance set and `REGION=&GRANT_ALIAS.PARAMETER1` is a parameterized object instance set. In the context of a specific object instance, grants specify the allowable actions on the set of accessible object instances. In the database, grants are stored in FND_GRANTS and object instance sets are stored in FND_OBJECT_INSTANCE_SETS. Object access can be tested using the privilege check application programming interface (API).

Securing a Business Object

A business object is a logical entity that is typically implemented as a table or view, and corresponds to a physical database resource. The data security policies of the security reference implementation secure predefined database resources. Use the Manage Data Security Policies task to define and register other database resources.

Data security policies identify sets of data on the registered business object and the actions that may be performed on the business object by a role The grant can be made by data instance, instance set or at a global level..

Note

Use parameterized object instance sets whenever feasible to reduce the number of predicates the database parses and the number of administrative intervention required as static object instances sets become obsolete. In HCM, security profiles generate the instance sets.

Data Role Templates: Explained

You use data role templates to generate data roles. You generate such data roles, and create and maintain data role templates in the Authorization Policy Manager (APM).

Note

HCM data roles are generated using the Manage Data Roles and Security Profiles task, which uses HCM security profiles, not data role templates, to define the data security condition.

The following attributes define a data role template.

- Template name
- Template description
- Template group ID
- Base roles
- Data dimension
- Data role naming rule
- Data security policies

The data role template specifies which base roles to combine with which dimension values for a set of data security policies. The base roles are the parent job or abstract roles of the data roles.

Note

Abstract, job, and data roles are enterprise roles in Oracle Fusion Applications. Oracle Fusion Middleware products such as Oracle Identity Manager (OIM) and Authorization Policy Manager (APM) refer to enterprise roles as external roles. Duty roles are implemented as application roles in APM and scoped to individual Oracle Fusion Applications.

The dimension expresses stripes of data, such as territorial or geographic information you use to partition enterprise data. For example, business units are a type of dimension, and the values picked up for that dimension by the data role template as it creates data roles are the business units defined for your enterprise. The data role template constrains the generated data roles with grants of entitlement to access specific data resources with particular actions. The data role provides provisioned users with access to a dimensional subset of the data granted by a data security policy.

An example of a dimension is a business unit. An example of a dimension value is a specific business unit defined in your enterprise, such as US. An example of a data security policy is a grant to access a business object such as an invoice with a view entitlement.

When you generate data roles, the template applies the values of the dimension and participant data security policies to the group of base roles.

The template generates the data roles using a naming convention specified by the template's naming rule. The generated data roles are stored in the Lightweight Directory Access Protocol (LDAP) store. Once a data role is generated, you provision it to users. A user provisioned with a data role is

granted permission to access the data defined by the dimension and data security grant policies of the data role template.

For example, a data role template contains an Accounts Payable Specialist role and an Accounts Payable Manager role as its base roles, and region as its dimension, with the dimension values US and UK. The naming convention is [base-role-name]:[DIMENSION-CODE-NAME]. This data role template generates four data roles.

- Accounts Payable Specialist - US (business unit)
- Accounts Payable Specialist - UK (business unit)
- Accounts Payable Manager - US (business unit)
- Accounts Payable Manager - UK (business unit)

Making Changes To Data Role Templates

If you add a base role to an existing data role template, you can generate a new set of data roles. If the naming rule is unchanged, existing data roles are overwritten.

If you remove a base role from a data role template and regenerate data roles, a resulting invalid role list gives you the option to delete or disable the data roles that would be changed by that removal.

Making Changes to Dimension Values

If you add a dimension value to your enterprise that is used by a data role template, you must regenerate roles from that data role template to create a data role for the new dimension. For example if you add a business unit to your enterprise, you must regenerate data roles from the data role templates that include business unit as a dimension.

If you add or remove a dimension value from your enterprise that is used to generate data roles, regenerating the set of data roles adds or removes the data roles for those dimension values. If your enterprise has scheduled regeneration as an Oracle Enterprise Scheduler Services process, the changes are made automatically.

For information on working with data role templates, see the Oracle Fusion Middleware Administrator's Guide for Authorization Policy Manager (Oracle Fusion Applications Edition).

7

Privacy

Privacy: Explained

Private data is data about individuals that should not be available to other individuals and organizations without specific business justification, even if it is in the possession of another party.
Individuals must be able to exercise a substantial degree of control over their private data and its use. Private and personal data includes the following.

- Personal information, such as date of birth, national identifier (SSN, NI number, and so on), marital status, gender, and passport, visa, or license numbers
- Contact details, such as home address, home phone number, and cell phone number
- Information about a person's contacts, such as family members and beneficiaries
- Lifestyle information or affiliations, such as ethnic origin, race, religion, sexual orientation, political allegiances, or drug testing data
- Medical information
- Compensation details, such as salary, bonus, or stock

An enterprise protects private and sensitive data against theft and misuse for the following reasons.

- Legal regulation
- Financial liability
- Customer expectation
- Brand risk

Privacy Attributes

One aspect of privacy is personally identifiable information (PII).
Oracle Fusion Applications security protects the following levels of data classification for addressing data privacy and protection requirements. The following table shows what protections are in place for which PII classifications.

PII Classification	Protected in Oracle Fusion Applications
Public	No
Public within the enterprise	User interface
Confidential	User interface and database

Unless otherwise stated, PII data in this discussion is confidential.
Public data is typically not sensitive with generally minimal risk associated with exposure of this information except in some contexts. For example, you may want to protect e-mail addresses from exposure to spammers or the names and titles of employees from access by external recruiters.

Internally public or confidential information is controlled to remain confidential within an entity and protected from access external to the entity such as a corporation.

Confidential data protects information within an entity such as a corporation. Exposure of such information outside the custodial entity is reasonably expected to result in harm, such as loss of business, benefit to a competitor, legal liability, or damaged reputation. Certain roles may require access to some confidential PII data for valid business reasons. For examples, a person's human resources representative probably has access to their home address, while a dispatcher may have access to the home phone numbers of on-call staff. However, this in no way alters the need for extra measures to protect sensitive PII data.

Oracle Fusion Applications uses Virtual Private Database (VPD) to protect PII attributes in the database from unauthorized access by privileged users such as database administrators (DBA). Data that is public or public within the enterprise, such as person name and work phone number, does not need the additional VPD protection.

Some privacy attributes are not PI,I but are sensitive. Oracle Fusion Applications uses Oracle Database Vault to protect all sensitive data from unauthorized access by privileged users such as DBAs, including VPD protections some DBAs may otherwise be powerful enough to override.

The following attributes are considered PII.

PII Attribute	Public: no additional security	Public within the enterprise: secure in the user interface	Confidential: secure in the user interface and database
Account Name		Yes	
Article Number			Yes
Bank Account Number			Yes
Biometrics Data			Yes
Business Address		Yes	
Business Email Address		Yes	
Business Telephone Number		Yes	
Card Number: Credit or Debit			Yes
Citizenship Number			Yes
Civil Identifier Number			Yes
Club Membership ID		Yes	
Custom Name	Yes (Recruiter in HCM Recruiting System)	Yes	
Digital ID			Yes
Drivers License Number			Yes
Electronic Taxpayer Identification Number			Yes
Employee Number	Yes (Recruiter in HCM Recruiting System)	Yes	
Government Affiliation ID			Yes
GPS Location		Yes	

Hafiza Number			Yes
Health Insurance Number			Yes
Identity Card Number		Yes	
Instant Messaging Address		Yes	
Library Card Number		Yes	
Maiden Name		Yes	
Mail Stop		Yes	
Medical Information			Yes
Military Service ID			Yes
National Identifier			Yes
Party Number or Customer Number		Yes	
Passport Number			Yes
Pension ID Number			Yes
Pension Registration Number			Yes
Person Identification Number			Yes
Person Name	Yes (Name of recruiter in HCM Recruiting System)	Yes	
Personal Address			Yes
Personal Email Address			Yes
Personal Public Service Number			Yes
Residency Number (Green Card)			Yes
Social Insurance Number			Yes
Social Security Number			Yes
Student Examination Hall Ticket Number		Yes	
Tax Registration Number or National Taxpayer Identifier			Yes
Trade Union Membership Number			Yes
Unemployment Insurance Number			Yes
User Global Identifier		Yes	
Visa Number or Work Permit			Yes
Voter Identification Number			Yes
Web Site		Yes	

Welfare Pension Insurance Number			Yes

These attributes participate in data security policies to prevent unauthorized access to the private data attribute values. Users are not always granted access to their own PII data. You provision roles and associated data security policies to grant access to a user's own PII data where it is necessary or cost effective to do so, such as for managing e-mail addresses.

The following data is sensitive, though not PII.

Sensitive Attribute Category	Public	Internal Public	Confidential Restricted	Confidential Highly Restricted	Type	Use
Unannounced Financial Results				Yes	Commercial	
Financial Forecasts				Yes	Commercial	
Competitive Analysis			Yes		Commercial	
Strategic Business Plans				Yes	Commercial	
Product design specifications				Yes	Commercial	
Compensation			Yes		Personal	Salary, bonus, stock, bank and account information, retirement accounts
Employment details			Yes		Personal	Performance evaluation, grade, ranking, hire date, background checks and security clearances
Nationality and Citizenship			Yes		Personal	Including work permit information
Health Information				Yes	Personal	Disability leave, health care providers and plans, medical information

Personal information				Yes	Personal	Birth date, place of birth, race and ethnicity, medical information, religion, politics, sexual orientation, union membership, offenses, race and ethnicity
Mother's maiden name				Yes	Personal	
Passwords				Yes	Security	Including access code or PIN
Encryption keys				Yes	Security	
Customer configuration				Yes	Security	
Security vulnerabilities				Yes	Security	

Data Privacy

Oracle Fusion Applications security protects private data from unnecessary external exposure through role based access controls and tools such as Virtual Private Directory (VPD) for access from remote locations.

Use the function and data security mechanisms of the Oracle Fusion Applications security approach to protect other sensitive data in your enterprise that is not considered PII. such as compensation information, medical information, or ethnicity, especially when associated with data that can identify the person the data belongs to.

Oracle Fusion Applications Payments secures credit card and bank account data using encryption, masking, hashing and compression at the application level, but the protection is enforced across all Oracle Fusion applications.

Business objects relevant to privacy and the data security policies defined to protect them are listed in the Oracle Fusion Applications Security Reference Manual for each offering.

Personally Identifiable Information: How It Is Processed

Personally identifiable information (PII) attributes in Oracle Fusion Applications span several product families.

- Financials
- Procurement
- Human Capital Management

Under most of the regulatory schemes (EU, Canada, Japan, and so on), PII includes all information from which the identity of a person could be determined directly or indirectly.

Attributes That Affect PII

The following attributes are considered PII in Financials.

- National Identifier Oracle Fusion Expenses
- Bank Account Number in Oracle Fusion Payments
- Card Number in Oracle Fusion Payments
- Tax Registration Number in Oracle Fusion Tax
- Tax Registration Number in Oracle Fusion Expenses
- National Taxpayer Identifier in Oracle Fusion Financials for EMEA
- National Taxpayer Identifier in Oracle Fusion Expenses

The following attributes are considered PII in Procurement.

- Internal Public
  - Supplier Address (business)
  - Supplier Telephone Number (business)
  - Supplier Email Address (business)
- Confidential
  - Supplier National Taxpayer Identifier
  - Supplier Tax Registration Number
  - Supplier Bank Account Number

The following attributes are considered PII in Human Capital Management.

PII	Confidential PII
Address	Private Address Details
Drivers License Number	Drivers License Number
	Private Email Details
Article Number	Article Number
Civil Identifier Number	Civil Identifier Number
Civil Registration Number	Civil Registration Number
GOSI Number	GOSI Number
Government Affiliation ID	Government Affiliation ID
Hafiza Number	Hafiza Number
Military Service ID	Military Service ID
National Identifier	National Identifier
National Taxpayer Identifier (NIP)	National Taxpayer Identifier (NIP)
Nationality Number	Nationality Number
Pension ID Number	Pension ID Number

Social Insurance Number	Social Insurance Number
Social Security Number	Social Security Number
	Personal Public Service Number
	RFC ID
Tax Registration Number or National Taxpayer Identifier	Tax Registration Number
Unemployment Insurance Number	Unemployment Insurance Number
Passport Number	Passport Number
Person Name	
Maiden Name	
Telephone Number	Private Phone Details
Iqama Number	Iqama Number
Visa Number	Visa Number
Visa Number or Work Permit	Visa Number or Work Permit

How PII Is Processed

The following table shows how specific PII attributes correspond to a business object and are processed.

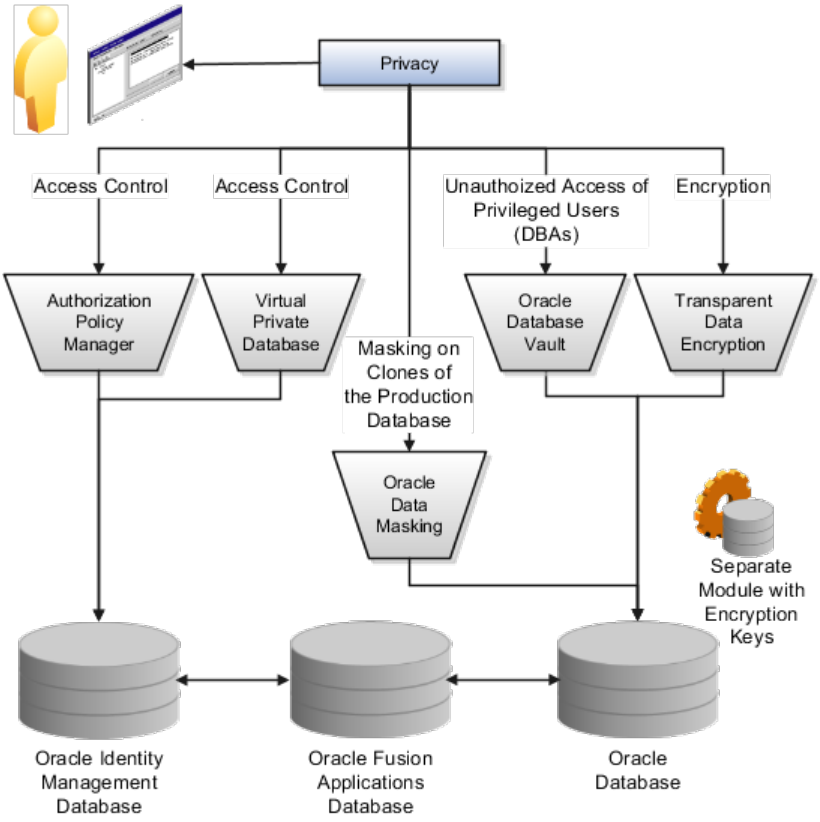
Data Attribute	Business Object	Comments
National Identifier Oracle Fusion Expenses	Corporate Card	Used to match new card not previously matched to employee
Bank Account Number in Oracle Fusion Payments	External Bank Account (LE)	Column subject to PCI/PABP in addition to PII security
	Disbursement (LE)	Masked payee bank account number, denormalized from IBY_EXT_BANK_ACCOUNTS_ALL; column subject to PCI/PABP in addition to PII security
	Disbursement (LE)	Masked payee bank account number, denormalized from IBY_EXT_BANK_ACCOUNTS_ALL; column subject to PCI/PABP in addition to PII security
Card Number in Oracle Fusion Payments	Payment Card (LE)	Column subject to PCI/PABP in addition to PII security
Tax Registration Number in Oracle Fusion Tax	Detail Tax Line (LE)	Tax Registration Number for external parties; may contain personal TRN
	Tax Registration (LE)	Tax Registration Number for external parties; may contain personal TRN. This attribute is indexed and search identifies non-equality.
	Party Tax Profile (LE)	Tax Registration Number for external parties; may contain personal TRN

Tax Registration Number in Oracle Fusion Expenses	Expense	Taxpayer Identifier of the merchant with which employee conducted the transaction
	Corporate Card Transaction	Taxpayer Identifier of the merchant with which employee conducted the transaction
National Taxpayer Identifier in Oracle Fusion Financials for EMEA	Spanish Withholding Interface (LE)	Supplier Taxpayer Identifier, used for Spanish Withholding Tax functionality
National Taxpayer Identifier in Oracle Fusion Expenses	Expense	Taxpayer Identifier of the merchant with which employee conducted the transaction
	Corporate Card Transaction	Taxpayer Identifier of the merchant with which employee conducted the transaction (column name may be sync up with previous entry)

Components That Protect PII

Several security components protect PII attributes.

The figure shows access controlled by Authorization Policy Manager and the Virtual Private Database protects PII data. Oracle Database Vault protects PII data from administrators. Transparent Data Encryption (TDE) protects PII in files. Oracle Data Masking protects PII data on clones of the production database.



Privacy attributes are listed in the Oracle Fusion Applications Security Reference Manual for each offering.

Privacy Safeguards: Points To Consider

In Oracle Fusion Applications, private data is accessed through user interfaces and client access tools such as SQL Plus.

Oracle Fusion Applications manages privacy by the following means.

- Oracle Virtual Private Database (VPD) protects personally identifiable information (PII) attributes other than the not sensitive public attributes such as name, work e-mail, work telephone, and so on.
- Oracle Transparent Data Encryption (TDE) stores private information in encrypted format in the database.
- Oracle Network Encryption encrypts private information on transit in the network or to monitor interfaces with outsourced service providers.
- Oracle Database Vault protects runtime account data from database administrators (DBA).
- Oracle Audit Vault enables auditing of privileged roles or activities.
- Oracle Data Masking and Oracle Fusion Data Security mask personal portions of data for non-authorized roles, where appropriate.

The following safeguards apply across Oracle Fusion Applications.

- Authentication
- Authorization

Oracle Fusion Applications security does not protect private data in onward transfers, or from one recipient to another. Network encryption protects sensitive data in transit.

Personally Identifiable Information (PII)

Oracle Fusion Applications secures personally identifiable information (PII) in the user interface and the database.

PII consists of attributes that are identified in the data model. PII attributes are degrees of sensitive. They can be confidential (such as taxpayer ID and credit card numbers) or not (such as person name and email address).

Role definitions carry authorization to access PII attributes. Data security policies define entitlement for a role to access PII attributes wherever they are stored or displayed. Network encryption provides protections of PII data in transit.

In Human Capital Management (HCM), Financials, and Procurement, Virtual Private Database (VPD) protects PII. Trading Community Architecture and

Oracle Fusion Payments uses Oracle Database Encryption APIs to secure confidential PII in their control at the column level, such as credit card and bank account numbers.

Oracle Transparent Data Encryption (TDE) prevents access to personally identifiable information (PII) in the file system or on backups or disk. Oracle Virtual Private Database (VPD) protects PII from users with DBA access, and Oracle Data Vault (ODV), if installed, prevents this protection from being overridden. Oracle Data Masking protects PII and sensitive data in cloned databases.

PII in interface tables used for custom integrations is not secured in the database, so needs to be secured at interfaces that are not in Oracle Fusion.

Sensitive Information

Information that is not PII but sensitive, such as compensation benefits and employee performance details, is protected through standard function and data security.

Notice and Consent

As a security guideline, publish the privacy policy for the enterprise. When collecting private or personal data, notify users how the data will be used and who can access it.

Privacy Breach Prevention and Recovery: Points To Consider

Breaches in privacy may occur due to the following issues.

- Failures in authentication
- Failures in storage
- Segregation of duties violations
- Customization and extensions
- Integrations with services that are not in Oracle Fusion

Privacy breaches could result also when data associated with a person is not masked even though all PII attributes are protected. For example, some combination of information a person's assignment, number of total or direct reports, and user account could allow a person's identity to be deduced.

Breach Prevention

The most effective measures preventing a breach of private data include the following.

- Oracle Fusion Applications security authentication and authorization
- Least privilege role definitions and provisioning
- Virtual Private Database (VPD) exclusion of private data from client access tools
- Oracle Database Vault exclusion of runtime account data from database administrator (DBA) access
- Encryption of PII attribute values
- Data masking

VPD security policies control database access at the row level. Only a SYS user or users can bypass VPD security policies with the EXEMPT ACCESS POLICY system privilege. Oracle Database Vault additionally prevents DBAs from accessing VPD protected data.

You can set up function security or row and column level data security using Oracle Fusion Data Security to secure private data, or set up Oracle Database Vault to restrict access through specified Internet Protocol (IP) addresses.

Recovery

Recovery from unauthorized access to private data depends on auditing and logging that identifies the privacy attributes breached without writing the private data to the log files or audit reports.

FAQs for Privacy

What's the difference between private, personally identifiable, and sensitive information?

Private information is confidential in some contexts.

Personally identifiable information (PII) identifies or can be used to identify, contact, or locate the person to whom the information pertains.

Some PII information is sensitive.

A person's name is not private. It is PII but not sensitive in most contexts. The names and work phone numbers of employees may be public knowledge within an enterprise, so not sensitive but PII. Under some circumstances it is reasonable to protect such information.

Some data is not PII but is sensitive, such as medical data, or information about a person's race, religion or sexual orientation. This information cannot generally be used to identify a person, but is considered sensitive.

Some data is not private or personal, but is sensitive. Salary ranges for grades or jobs may need to be protected from view by users in those ranges and only available to senior management.

Some data is not private or sensitive except when associated with other data the is not private or sensitive. For example, date or place of birth is not a PII attribute because by itself it cannot be used to uniquely identify an individual, but it is confidential and sensitive in conjunction with a person's name.

8

Enforcement Across Tools, Technologies, Data Transformations, and Access Methods

Enforcement Across Tools, Technologies, Data Transformations, and Access Methods: Explained

The security infrastructures of a Oracle Fusion Applications deployment vary from one tool in the technology stack to another, however the security approach coordinates transactional and analytical security so that all security policies and controls prevail across access methods to enterprise information and transformations of enterprise information.

Oracle Fusion Applications enforces each single statement of security policy through the multiple transformations of data necessary for transactions, dimensional analysis, and search optimization.

Oracle Fusion Applications are secure no matter which technology accesses information during implementation, deployment, and maintenance.

The Oracle Fusion Applications technology stack addresses the following risks to security.

- Complex combination of tools
- Various technologies used by those tools
- Transformations of data
- Multiple access methods
  - User interfaces
  - Transactions across products
  - Batch processes
  - External Web services

Enforcement Across Implementation Changes

Oracle Fusion Applications tools and technologies respect the security of your implementation or configuration across the changes you make to the deployment.

The changes you are likely to make involve the following:

- Role definitions
- Role provisioning
- Data security

For example, if you remove the Accounts Payable Manager enterprise role from the roles provisioned to a user, the user should not be able to gain access to any of the resources that are provisioned by the Accounts Payable Manager role. Similarly, if you have provisioned a user with only the Accounts Payable Specialist role, the user should only have access to the resources provisioned by the Accounts Payable Specialist role.

The heat map shows the ease of support from Oracle in assisting enterprises using the tools involved in reference implementation changes, where 1 is easiest and 7 most difficult. Application Development Framework represents the Oracle Fusion Applications user interface pages.

Summary Ease of Use	Tool					
Change	Application Development Framework (ADF)	Enterprise Scheduling Systems	Hyperion SmartView	Oracle Business Intelligence	Universal Content Management	Web Center
New Job With Existing Duties	1	1	1	1	1	1
New Job With New Duties	2	2	2	4	1	4
Existing Duty Change to Existing Entitlement	3	3	3	3	1	3
New Duty With Existing Entitlement	3	3	3	4	1	4
Existing Duty With New Entitlement	4	4	4	4	1	4
New Duty With New Entitlements	4	4	4	4	1	4
Existing Entitlement With Existing Permissions	5	5	5	5	1	5
New Entitlement With Existing Permissions	6	6	6	6	1	6
New Entitlement With New Permissions	7	7	7	7	1	7

Oracle Fusion Applications includes a predefined data warehouse with some but not all dimensions secured. For example the department dimension is secured. A packaged goods enterprise with branding managers can enable security on branding resources in the product dimension. While there are no such policies predefined in the Oracle Fusion Applications reference implementation, creating such polices enforces security respected by the product dimension in the data warehouse.

Enforcement Across Access Methods

Oracle Fusion Applications users access functions and data by the following means under the protection of their provisioned security policies.

- Menu navigation
- Worklists
- Global area recent items and favorites
- Oracle Fusion Search
- Analytics
- Tag clouds
- Oracle Enterprise Scheduler jobs
- Service Oriented Architecture (SOA) business flows (Business Process Execution Language (BPEL))

Enforcement Across Tools and Technologies: Points to Consider

Oracle Fusion Applications enforces security across the tools and technologies of the Oracle Fusion Applications technology stack. The Oracle Fusion Applications security approach is in effect in all tools and technologies used by Oracle Fusion Applications.

Oracle Fusion Applications uses the following tools and technologies.

- Oracle WebCenter Content
  - Tags
  - Watch list
- Search
  - Oracle Fusion Search
  - Enterprise Crawl and Search Framework (ECSF)
- Oracle Business Intelligence Foundation Suite
  - Oracle Business Intelligence Applications
  - Oracle Fusion Transactional Business Intelligence
  - Oracle Business Intelligence (BI) Publisher
- Oracle Enterprise Management
  - Oracle Enterprise Scheduler
  - Hyperion Enterprise Performance Manager (EPM)

- Applications Security
  - Lightweight Directory Access Protocol (LDAP)
  - Oracle Identity Manager
  - Oracle WebCenter Content Server
  - Service Oriented Architecture (SOA) business flows (Business Process Execution Language (BPEL))
  - Application Development Framework (ADF)
- Database Security
  - Extended Spread Sheet Database (ESSbase)
  - Hyperion SmartView
  - Oracle Virtual Private Directory (VPD)
  - Oracle Data Integrator (ODI)
  - Oracle Database 11g

Oracle WebCenter

Oracle Fusion Applications security enforcement across tools and technologies includes tags, and Watchlist in Oracle WebCenter.

The Application Development Framework (ADF) security framework handles authentication in Oracle WebCenter.

Tags

An Oracle WebCenter tag is a bookmark with user-defined keyword attributes that allow easily and repeatedly finding business objects. Tags are private or shared (public). A business object that is Oracle Fusion Search enabled can be tagged, but tagging a business objects does not make it search enabled. Users rename or delete their tags in the context of a specific resource using the tagging popup for the resource from where the tag first originated. Oracle WebCenter does not provide a user interface to users or administrators for managing all tags.

Tags in the cloud are sized according to the count of authorized documents.

Oracle Fusion Data Security secures database resources used with Oracle WebCenter tags. Oracle Fusion security enforces data security policies on the tags of each business object that is enabled for tagging. For example, Cost Center managers can view all purchase orders charged to their cost center and any tags to purchase orders that they have created or are publicly available.

Search

Oracle Fusion Applications security enforcement across tools and technologies includes Oracle Fusion Search and Enterprise Crawl and Search Framework (ECSF).

Oracle Fusion Search is enabled on searchable business objects. If a user is entitled to view a business object in Oracle Fusion Applications, then that user can search against the business object in Oracle Fusion Search. For example, the Manage Warehouse Shipments privilege protects the Manage Warehouse Shipments task flow. The view permissions of the same privilege allow searching against the View Object that corresponds to the searchable business object Shipment Request.

Oracle Fusion Search enforces access entitlement to the data source being searched. Oracle Fusion Applications applies data security policies to search results.

The Oracle Fusion Search index does not contain personally identifiable information (PII) data. Non-PII private and sensitive attributes contained in the search index for search are protected by standard data security mechanisms

Oracle BI and Oracle BI Publisher

Oracle Fusion Applications security enforcement across tools and technologies includes Oracle Business Intelligence Applications, Oracle Fusion Transactional Business Intelligence, and Oracle BI Publisher of the Oracle Business Intelligence Foundation Suite.

Oracle Fusion Applications data security policies protect dimensional analysis derived from transaction tables and data transformations. Analysis filters data according to the security policies that apply to the analyst's role.

Oracle BI Foundation Suite

Single Sign On (SSO) handles authentication in the Oracle Business Intelligence Foundation Suite.

Both function and data security applies to Oracle BI Applications and Oracle Fusion Transactional BI equally. These BI products use the Oracle BI Foundation security model to secure data. Oracle BI Foundation View Objects are subjected to the protections of data security policies through Oracle Fusion Data Security.

Oracle BI Foundation Suite uses Oracle Fusion Applications job and abstract roles and synchronize with application roles from Oracle Platform Security Service (OPSS). Duty roles entitle access to Oracle BI Foundation Subject Areas, Presentation Catalogs, Presentation Tables, Folders, Reports and Dashboards. In duty role hierarchies, the parent duty role provides assured revocation.

Virtual Private Database (VPD) policies secure personally identifiable information (PII) attributes in the Online Transaction Processing (OLTP) database.

Oracle BI Foundation Suite rarely collects metrics based on PII attributes. An extract, transfer, load (ETL) process enforces Online Transaction Processing (OLTP) Virtual Private Database (VPD) policies to protect exposed PII attributes.

Oracle Business Intelligence Foundation Suite masks data by first masking Online Transaction Processing (OLTP) and then running the BI extract, transfer, load (ETL) scripts that populate the BI warehouse. Since the ETL is run on a masked OLTP database, the data is masked in BI.

Oracle Fusion Transactional BI

Oracle Fusion Applications uses Oracle Fusion Transactional BI for real-time operational reporting. Your enterprise can create ad hoc queries against the transactional Oracle Fusion applications schema to report the current state and analysis of your operations. Oracle Fusion Transactional BI serves as the content source (View Objects) for Oracle Fusion Applications embedded graphs, which are secured by the Oracle BI Foundation security model.

Oracle BI Publisher

The ADF Security framework handles authentication in Oracle BI Publisher. Oracle Platform Security enforces function security in Oracle BI Publisher. Duty roles entitled provisioned users with access to Oracle BI Publisher reports. Since the Oracle BI Publisher report prepares report data using an Oracle Enterprise Scheduler job (batch process), the privilege that secures the Oracle Enterprise Scheduler job also grants access to the report.

Data security policies protect Oracle BI Publisher content. All users provisioned with the Worker role can consume the Oracle BI Publisher generated reports to which they are authorized. However, for access to modify the layout and formatting of the report, users also must be provisioned with the BI Author role by means of their Oracle Fusion Transactional BI and Oracle BI Applications subject areas.

Oracle BI Publisher reports may expose PII data. Data security policies secure folders in which Oracle BI Publisher groups reports that expose PII data.

For creating or editing data models in Oracle BI Publisher, users must be provisioned with a role that is entitled with a privilege that includes the oracle.bi.publisher.developDataModel permission. While the BI Administrator role is so entitled, this role grants such broad access that it may not be prudent to provision it to users. Instead, create a new custom role that provides the entitlement of the BI Author role and additionally grants the oracle.bi.publisher.developDataModel permission.

Enterprise Management

Oracle Fusion Applications security enforcement across tools and technologies includes Oracle Enterprise Manager, Oracle Enterprise Scheduler Service, and Hyperion Enterprise Performance Manager (EPM).

Oracle Enterprise Scheduler Service

Single Sign On (SSO) handles authentication in Oracle Enterprise Scheduler Service of the submitter of the job. Only authenticated users can submit Oracle Enterprise Scheduler jobs. For example, if user teller1 submits an Oracle Enterprise Scheduler job, the requested job runs as teller1 and is secured according to the provisioned roles and credentials of teller1.

Oracle Enterprise Scheduler Service uses the Oracle Platform Security Service (OPSS) and secures its components using OPSS permissions. Oracle Fusion Applications embeds Oracle Enterprise Scheduler Service components in the consuming application or invokes Oracle Enterprise Scheduler Service APIs and

services. The consuming application grants permission on the enclosing task flow to grant access to Oracle Enterprise Scheduler Service submission requests.

Identity propagates throughout the entire life cycle of an Oracle Enterprise Scheduler job. When an Oracle Enterprise Scheduler job needs to access data to which the submitter is not entitled, the job is defined to run under an application identity that carries elevated privileges.

Oracle Platform Security Services (OPSS) enforce function security in Oracle Enterprise Scheduler Service at the level of the submitting task flow. Access at the global level in Oracle Enterprise Scheduler Service secures the job with the View Batch Jobs privilege provisioned to the Worker role. Duty roles carry entitlement to perform Oracle Enterprise Scheduler tasks. Oracle Enterprise Scheduler Service also provides security on the metadata of a job, so Oracle Enterprise Scheduler permissions control the job or job set submission.

Data security policies secure database resources used with Oracle Enterprise Scheduler Service. An Oracle Enterprise Scheduler job accesses data that the submitting user is entitled to access or that the submitting application is entitled to access if the user's access is too limited. Submitting user information accompanies Oracle Enterprise Scheduler jobs for auditing purposes. Oracle Enterprise Scheduler jobs run using application identity will retain submitting user information also for auditing purpose as part of the payload. Application identity is part of Oracle Enterprise Scheduler job metadata definition.

If an Oracle Enterprise Scheduler job needs access to PII attributes, the user submitting the Oracle Enterprise Scheduler job, or the application identity running the Oracle Enterprise Scheduler job must have access to those PII attributes.

EPM

Oracle Access Manager handles authentication in Hyperion Enterprise Performance Manager (EPM).

EPM enforces function security in cube access managed through Extended Spread Sheet Database (ESSbase) Server. Access to ESSbase Server provides access to all cubes in that server. Permissions in Oracle Fusion Applications roles correspond to EPM roles.

ESSbase uses data security policies. EPM enforces data security with security filters on each cube in ESSbase.

PII attributes are not present in EPM.

Applications Security

Oracle Fusion Applications security enforcement across tools and technologies includes LDAP, Oracle Identity Manager, HCM security profiles, Oracle WebCenter Content, and Application Development Framework (ADF).

Oracle WebCenter Content

Oracle WebCenter Content uses SSO to authenticate access to the Content Server. When a user accesses Oracle Fusion Applications, the user's identity propagates to Oracle WebCenter Content. Security policy enforcement in Oracle WebCenter

Content extends only to attachments on Oracle Fusion Applications objects, not to all content stored by Oracle WebCenter Content.

When user attaches a file to an object within the Oracle Fusion Applications, they can choose to mark the file as Shared or Not Shared. By default, text and file type attachments related to applications data are not shared and can only be viewed in Oracle Fusion Applications user interfaces. Oracle WebCenter Content user interfaces only gives access to shared files.

Note

Set the `repositoryMode` property to true to show the Shared column in the Attachments table.

Access to the owning table, such as for purchase orders, agreements, supplier accounts, and so on, secures the attachments. For example, by default a role that has access to the purchase order can see ALL attachments for the purchase order. As a result, users only have access to documents attached to data to which they are authorized. If a document is not viewable in the transaction system, it is also not viewable in the Content Management System

Access to attachment category additionally may secure attachments. For example, employee tax reports, payslips, and visa details are each attachment categories. Each employee can see their tax reports and payslips. A payroll professional user can see the tax reports for the people they manage but not visa details for those workers. An HR professional user can see the visa details for workers they are managing, but not payslips and tax reports for those workers.

If attachments are categorized, access may be secured by attachment category. In Procurement, data grants are based on attachment categories. For example, the Procurement Applications Administrator can only access attachments in attachment categories owned by Procurement.

Document Type security profiles protect attached HCM documents.

Data security policies protect access to privacy data based on Document Category.

ADF

Application Development Framework (ADF) is a framework of design pattern implementations and metadata-driven components used to build the Java EE Oracle Fusion Applications. ADF includes business components and faces, Web Services and attachments. ADF uses the Oracle Platform Security Service (OPSS).

The ADF instance running Oracle Fusion Applications supports the following security enforcement.

- User authentication using Oracle Single Sign On (SSO)
- Function security authorization using Oracle Platform Security Services (OPSS)
- Data security authorization using Oracle Fusion Data Security
- Privacy

Oracle Fusion Data Security are used to secure database resources used with ADF and Web Services. Data security relies on the FND session to be properly initialized. The session initialization takes the user and role information from the security subject and stores it on the session. Data security uses the information from the session when deciding whether a user is authorized to access the data.

A common set of enterprise roles secures functions for Oracle Fusion Applications across all tools and technologies.

Database Security

Oracle Fusion Applications security enforcement across tools and technologies includes Extended Spread Sheet Database (ESSbase), Hyperion SmartView, Oracle Database 11g, Oracle Data Integrator (ODI), and Virtual Private Directory (VPD).

SSO handles authentication in ESSbase, which accesses Hyperion SmartView on a client machine.

Oracle Fusion Applications security enforces function security on the ESSbase server, not separately on ESSbase cubes. Queries on an ESSbase cube access members of dimensions, such as business units and projects, that are authorized by Online Transaction Processing (OLTP).

Predefined duty roles that carry the EPM Admin permission provide administration access for all cubes in the server. Predefined duty roles that carry the EPM Filter permission provide read-only access to all cubes in the server and authorize view access to View Objects in SmartView.

Filters define which dimensions ESSbase secures. Data security policies enforce data access security on data stored within Essbase. SmartView in Excel and Financial Reporting access ESSbase and enforce data security policies defined with filters.

Changes to Oracle Fusion Applications data security through changes in role provisioning or data security policies propagate to ESSbase for each Oracle Fusion Applications session at the time the session is created and not through periodic synchronization.

PII attributes are not present in ESSbase.

Security Across Access Methods: How It Is Enforced

Oracle Fusion Applications enforce security across various access methods.

Access Methods That Preserve Function and Data Security

The following access methods preserve the defined security of Oracle Fusion Applications functions and data.

- Oracle Fusion Applications user interfaces
  - User sign on
  - User navigation
  - Scheduled processes
- Oracle Business Intelligence Foundation Suite for Oracle Applications
- BI Publisher
- External Web services

Authorization policies across all tools and technologies align with the Oracle Fusion Applications enterprise roles.

The following access methods in Oracle Fusion Applications are subject to entitlement, approvals, and policies.

- Menu navigation where navigation paths are subject to an entitlement
- Worklists where worklist content is subject to a privilege
- Oracle Fusion Search where the data source is subject to a privilege and security policies have been applied to the results
- Imbedded analytics where the data is filtered according to security policies that apply to a role
- Tag clouds where a tag in the cloud is sized according to a count of authorized documents

These access methods are a valid way to access the data that you need and all respect the same security policies.

How Access Security Is Enforced

Access security is enforced using the features of the Oracle Fusion Applications security approach.

Enforcement Details

Specific enforcement details apply to the following access methods.

- Single sign on (SSO)
- Navigation paths
- Scheduled processes

Single Sign On

The Application Development Framework (ADF) instance running Oracle Fusion Applications supports SSO user authentication. Oracle Fusion Applications uses Oracle Access Management (OAM) for SSO.

The Policy Manager in Oracle Access Management supports the administrative tasks necessary to manage SSO and URL-based authentication and authorization policies. These policies have no relationship with OPSS policies that handle function security authorization.

SSO handles authentication in the following tools and technologies accessed by Oracle Fusion Applications.

- Oracle Business Intelligence Foundation Suite for Oracle Applications
- Oracle Enterprise Scheduler
- Oracle WebCenter Content
- Extended Spread Sheet Database (ESSbase)
- Hyperion SmartView

With SSO, a user who accesses a protected resource without having a current session cookie in the browser is redirected to the SSO server for authentication. Upon successful authentication, SSO places a session cookie in the user's browser cache.

Navigation Paths

Many targets are accessed through multiple navigation paths and roles. Oracle Fusion Applications tools and technologies secure the targets of access regardless of which navigation path is used.

Entitlement privileges secure navigation paths. For example, the common component Create Item securing the business process management (BPM) task Create Items must be navigated from different Work Areas based on the roles that execute the task.

User Type	Job Role	Navigation to Work Area (Path)	BPM Task
Producer	Product Manager	Product Management > Items	Create Item
Consumer	Warehouse Manager	Warehouse Operations > Inventory	Create Item
Consumer	Cost Accountant	Costing > Cost Accounting	Create Item

In the above example, for a user provisioned with the Product Manager role, the Create Item task should appear in the Items work area under the Product Management navigation path, whereas a user provisioned with the Warehouse Manager role should see the Create Item task in the Inventory work area under the Warehouse Operations navigation path.

Oracle Enterprise Scheduler Services Processes

Function and data security policies protect batch jobs.

Enforcement of Security Policies: Points To Consider

Across the tools of the Oracle Fusion Applications deployment, the technologies may differ, but the Oracle Fusion Applications security approach enforces all security policies.

Oracle Fusion Applications security policies are respected in all tools and access methods.

- Transactions
- Analytics
- Search
  - Oracle Fusion Applications data
  - Tag cloud

Note

With the exception of queries on personally identifiable information (PII) that are secured in the database through Virtual Private Database (VPD) policies, direct queries against the database are not secured.

For example, a manager is entitled through the privileges of provisioned roles to see expenses submitted by their direct reports. The manager sees the expenses in the expense review transactions, in the expense analytics transaction, through Oracle Fusion Search and through tag cloud navigation. The manager is not able to see expenses submitted by people who do not work for them and is prevented from seeing expenses not submitted by direct reports.

A manager sees expenses charged to their own cost center and any cost center managed by a person who reports to the manager.

Transactions, analytics, enterprise or tag navigation searches, and ad hoc queries consistently enforce security policies.

For example, if an information resource such as a purchase order is subject to the access policy that "Buyers can see purchase orders for the business units for which they are the authorized buyer," this data security policy applies to a user with that role regardless of the route the access takes, such as in metrics through Oracle Business Intelligence Foundation Suite for Oracle Applications (OBIFA), in searches through Oracle Fusion Search, or in a business function through Oracle Fusion Applications.

Oracle Fusion Applications enforces access policies on the original transaction table, as well as on data transformations for dimensional analysis. For example, in reviewing payables transactions, an Accounts Payables Manager is able to view invoices by performing the View Accounts Payable Transactions action for the business units for which they are authorized. While performing the Accounts Payable Invoice Analysis action, the Accounts Payables Manager is able to analyze payables invoices for the business units for which they are authorized. An Accounts Payable Manager is able to view the same payables

invoices whether they are reviewing payables invoices in the transactional system or analyzing payables invoices in the analytical system.

Oracle Platform Security Services (OPSS) and data security policies secure functions and data across technologies, such as ADF Entity Objects, View Objects, Page Definitions and Bindings, and search indexes securing Oracle Business Intelligence, Extended Spread Sheet Database (ESSbase), Oracle WebCenter, and tag clouds.

Function Security

The securing technologies of Oracle Business Intelligence Foundation Suite for Oracle Applications (OBIFA) security and Oracle WebCenter authorization implement function security policies. Oracle Platform Security Services (OPSS) handles function security authorization across all tools and technologies.

View transaction privileges control view transactions across all technologies. Each privilege to secure a single real world action alone controls that action across all technologies. No other privilege secures that real world action.

Data Security

The securing technology of Oracle Fusion Data Security, security plugins, and filters implement data security policies. Oracle Fusion Data Security handles data security authorization across all tools and technologies.

Documents that are not viewable in the transaction system are also not viewable in the Content Management System

Privacy

The standard data security mechanisms across all Oracle Fusion Applications technology, tools, and access methods enforce security policies protecting privacy. Additional security mechanisms protect sensitive PII data.

PII data is not moved or transformed to less secure technologies. For example, PII data is not passed to Lightweight Directory Access Protocol (LDAP) stores. If an Online Transaction Processing (OLTP) application is the source of the PII data, it is not passed to Oracle Business Intelligence Applications for exposure in metrics. If a non-OLTP application is the source of the PII data, it is passed to Oracle BI Applications using extract, transfer, and load (ETL).

Identity and Access Provisioning

Oracle Identity Management (OIM) handles user and role provisioning across all tools and technologies. Oracle Fusion Applications security uses enterprise role and Oracle Identity Management to control access across all tools and technologies. All enterprise roles in Oracle Fusion Applications align with authorization policies across all tools and technologies.

Oracle Fusion Applications distinguishes between user identities and application identities (APPID). Predefined application identities serve to authorize jobs and transactions that require higher privileges than users.

Segregation of Duties

Segregation of duties policies are enforced in all tools and access methods.

The Security Reference Implementation

Oracle Fusion Applications consistently respects and enforces all security policies in the security reference implementation.

The security reference implementation can be viewed in the user interfaces where security tasks are performed or in the security reference manual (SRM) for each Oracle Fusion Applications offering.

9

Segregation of Duties

Segregation of Duties: Explained

Segregation of duties (SOD) separates activities such as approving, recording, processing, and reconciling results so an enterprise can more easily prevent or detect unintentional errors and willful fraud. SOD policies, called access control policies in Application Access Controls Governor (AACG), exert both preventive and detective effects.

SOD policies constrain duties across roles so that unethical, illegal, or damaging activities are less likely. SOD policies express constraints among roles. Duty role definitions respect segregation of duties policies.

Application Access Controls Governor

You manage, remediate, and enforce access controls to ensure effective SOD using the Application Access Controls Governor (AACG) product in the Oracle Enterprise Governance, Risk and Compliance (GRC) suite.

AACG applies the SOD policies of the Oracle Fusion Applications security reference implementation using the AACG Oracle Fusion Adapter.

AACG is integrated with Oracle Identity Management (OIM) in Oracle Fusion Applications to prevent SOD control violations before they occur by ensuring SOD compliant user access provisioning. SOD constraints respect provisioning workflows. For example, when provisioning a Payables role to a user, the SOD policy that ensures no user is entitled to create both an invoice and a payment prevents the conflicting roles from being provisioned. AACG validates the request to provision a user with roles against SOD policies and provides a remediating response such as approval or rejections if a violation is raised.

Use AACG to for the following.

- Define SOD controls at any level of access such as in the definition of an entitlement or role.
- Simulate what-if SOD scenarios to understand the effect of proposed SOD control changes.
- Use the library of built-in SOD controls provided as a security guideline.

Managing Segregation of Duties

SOD policies express incompatible entitlement or incompatible access points into an application. In GRC, an access point is the lowest level access for a particular application. In GRC, entitlement is a grouping of access points. As a security guideline, group the lowest level access points or define the SOD policy at the access level causing the least amount of change. Business activities are enabled at access points. In Oracle Fusion Applications, the hierarchy of access points in descending levels is users, roles, and entitlement.

Note

AACG entitlements are logical groupings of security objects that represent Oracle Fusion Application access points such as roles or entitlement.

Note

In AACG, segregation of duties policies are called access controls.

Oracle Fusion Applications does not predefine business logic for dealing with SOD conflicts. Oracle Fusion Applications does define a set of states where role requests are suspended pending resolution of SOD violations the role request introduces. In most cases, Oracle Fusion Applications invokes OIM to handle role requests. Enterprises define SOD resolution rules when defining SOD policy.

Remediating Segregation of Duties Policy Violations

The risk tolerance of your enterprise determines what duties must be segregated and how to address violations.

AACG assists in remediation of violations with a guided simulation that identifies corrective action. You determine the exact effects of role and entitlement changes prior to putting them into production, and adjust controls as needed.

For information on managing segregation of duties, see the Oracle Application Access Controls Governor Implementation Guide and Oracle Application Access Controls Governor User's Guide.

Defining Segregation of Duties Policies: Points To Consider

Segregation of duties (SOD) policies express incompatibilities enforced to control access in defined contexts.

In Oracle Fusion Applications, SOD policies protect against the following incompatibilities.

- Privilege X is incompatible with privilege Y
- Role A is incompatible with role B
- Any privileges in role A are incompatible with any privileges in role B.
- Privilege X is incompatible with any privileges in role B.

The following examples of SOD policies illustrate incompatible entitlement.

- No user should have access to Bank Account Management and Supplier Payments duties.
- No user should have access to Update Supplier Bank Account and Approve Supplier Invoice entitlement.

Data Contexts

You can extend SOD policies to control access to specific data contexts.

For example, no single individual must be able to source a supplier in a business unit and approve a supplier invoice in the same business unit.

Exclusion and Inclusion Conditions

SOD policies may include exclusion conditions to narrow the SOD scope and reduce false positive violations, or inclusion conditions to broaden the scope.

Conditions apply to access points globally, to policies, or to access paths defined by policies. Access path conditions can exclude a user from a role, an Oracle Fusion Applications entitlement from a role, or a permission from an Oracle Fusion Applications entitlement.

The following global exclusion conditions are predefine in Oracle Fusion Applications and available when creating SOD policies.

- User Status
- User Name
- Enterprise Role
- Action
- Business Unit
- Within Same Business Unit

Enforcement

Oracle Fusion Applications enforces SOD policies under the following circumstances.

- When granting entitlement to a role
- When provisioning a role to a user

For information on managing segregation of duties, see Oracle Application Access Controls Governor Implementation Guide and Oracle Application Access Controls Governor User's Guide.

Note

SOD policies are not enforced at the time of role definition.

A single SOD policy can include entitlement from multiple instances of a single enterprise resource planning environment. For example, one SOD policy is enforced in implementation, test, and production instances of Oracle Fusion Applications.

Managing Segregation of Duties Risks and Violations: Critical Choices

You assess and balance the cost of duty segregation against reduction of risk based on the requirements of your enterprise.

The types of people who resolve SOD conflicts include the following.

- Administrator of an external program such as the Procurement Administrator for the supplier portal or the Partner Manager for the PRM Program
- Senior executive spanning multiple organizations in an enterprise with opposing interests
- Risk management professional implementing an Oracle Enterprise Governance, Risk and Compliance (GRC) initiative
    - Predefines a set of conditions and informs access provisioning staff to approve requests and prove the exception based on certain conditions
    - Allows defining rules to route SOD violations for approval

You view and respond to risks and violations in the Application Access Controls Governor (AACG).

You may wish to override an SOD violation. For example, the Accounts Payable Supervisor includes incompatible duties to create both invoices and payments. When you provision this job role to a user, you may waive the violation in the AACG. You may waive the violation for the currently provisioned user, for the SOD policy that raised the violation, or for the SOD policy within a particular data set, such as a business unit.

The risk tolerance of your enterprise guides how you respond to conflicts. For example, a user may be provisioned with both the role of Order Manager and

Shipping Agent. The Order Manger role entitles the user to enter orders, which could result in exploitation when filling shipping quotas. You can remove the entitlement to enter orders that the Order Manger job role inherits from the Orchestration Order Scheduling Duty role. Or you could segregate the shipping and order entry duties by defining an SOD policy that allows a user to have either job role but not both.

False Positives

False positives can be SOD policy violations that are not actually violations, or are violations within your risk tolerance and therefore do not require corrective action.

You can reduce false positives by the following methods.

- Define exclusion conditions that can be applied to individual or groups of policies.
- Define logically complex SOD policies that enforce more exacting specifications.
- Determine whether conflicts should be prevented, monitored, or subjected to approval during provisioning.

Path Level Detection

Conflict analysis detects a user's multiple paths to one or more conflicting access points.

For example, a user may be able to reach a single access point through one or more roles, or by one entitlement leading to another through submenus to a function that represents a risk. The resulting conflict path shows if the conflict is generated by inappropriate role provisioning or configuration of applications. The audit shows the paths from any number of users to any number of access points involved in conflicts, which lets you visualize the root cause and remediate effectively.

AACG assigns one or more users to review all paths involved in a given conflict so that the entire conflict can be addressed in a coherent way.

Waiving or Accepting Violations

AACG lets you accept or waive a violation. Your reasons may include that you accept the risk or will define compensating controls.

A waiver may apply to the current user, constraint, or constraint within a dimension such as the business unit.

Resolving Conflicts

The risk tolerance of the enterprise determines whether a segregation of duties conflict must be removed from the security reference implementation.

The following approaches resolve conflicts.

- Change the segregation of duties policy.
- Ensure a job role does not contain incompatible duties.
- Define data security policies that restrict authorized access by incompatible duties.

Changing a segregation of duties policy may not be possible in most cases. For example, a policy that segregates creation of payables invoice from making payables payments should be preserved, even if the Accounts Payables Manager job role includes a duty role for each activity. To prevent an accounts payables manager from being authorized to perform both duties, or from being authorized to make payables payments to self and direct reports, the Accounts Payables Manager job role must be changed. The security implementation can be changed to include two job roles that segregate the incompatible duties. Added data security policy grants can restrict the access to at risk data.

For information on managing segregation of duties, see the Oracle Application Access Controls Governor Implementation Guide and Oracle Application Access Controls Governor User's Guide.

10

Identity Management and Access Provisioning

Identity Management and Access Provisioning: Explained

You provision identities with access through user accounts, roles, and role memberships. Users should have resources and access rights based on their job or position within the enterprise.

User accounts are created as identities and stored in the Lightweight Directory Access Protocol (LDAP) store. Oracle Fusion allows direct integration with any LDAP server. Roles are provisioned by making the identity a member of a group that is the requested role. Roles are automatically provisioned based on the assignment of the employee. Authorized users are provisioned into the Oracle Fusion database as needed.

Resources such as identities or accounts, enterprise roles, and application roles are provisioned and reconciled based on policies.

HCM processes, such as for a new hire or transfer, trigger identity management and access provisioning.

Identity Management

Oracle Identity Management (OIM) is available in Oracle Fusion Applications through integration with Oracle Fusion Middleware. Identity management in Oracle Fusion Application involves creating and managing user identities, creating and linking user accounts, managing user access control through user role assignment, managing workflow approvals and delegated administration. An example of delegated administration is a sales line of business approving access to sales roles, rather than having the IT security manager approve such access.

In addition to using OIM pages in Oracle Fusion Applications, you can provision users with access to functions and data through various product features, such as team definitions in Oracle Projects.

Oracle Fusion Applications and applications not in Oracle Fusion Applications may share OIM for identity management.

Access Provisioning

Oracle Fusion Applications notifies the IT security manager of the account requests, role provisioning requests, and grants to ensure role administration is always documented, authorized and auditable.

Most Oracle Fusion applications use events within applications to start the provisioning activities. Most of these provisioning events are concerned with users that are part of the enterprise that is deploying the application, but there are also many users that may not be part of the deploying enterprise, such as applicants, account managers that work for your suppliers, or project team members that work for consulting agencies.

Role provisioning events occur across the life cycle of your implementation and deployment.

- Employees, contingent workers, internal users
  - Hiring
  - Self-service role requests
  - Transfers, moves, and reorganization
  - Termination
- Suppliers, partners, external users
  - Registering account managers and support representatives
  - New role request, such as joining a new partner program
  - Change in procurement policy triggers reevaluation of role membership
    - Prospective supplier requests user account during supplier registration or existing supplier requests accounts for additional employees
    - Parent organization's program structure changes and creates need for role revocation or creation of additional roles
  - Scheduled role provisioning request triggers role provisioning at a future effective date and time

Provisioning additional roles to employees or internal users may cause an segregation of duties (SOD) violation with already provisioned roles. In contrast, provisioning roles to external users such as partners or suppliers is not likely to cause an SOD violation for individuals but may cause an SOD conflict for the host enterprise.

In most cases, Oracle Fusion Applications invokes OIM to handle role requests and role provisioning. The PER_USER_ROLES table stores information about what roles are provisioned to which users.

Note

Use Oracle Identity Management (OIM) to configure audits of provisioning events.

Tip

As a security guideline, avoid having users entitled to provision roles from being the same users who are defining those roles.

For more information about Oracle Internet Directory as the Lightweight Directory Access Protocol (LDAP) server, see Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory.

Securing Identities and Users: Points To Consider

Identity covers all aspects of an entity's existence within the contexts in which it is used. The identity of an enterprise user consists of HR attributes, roles, resources, and relationships.

HR attributes include identifying information about a user that is relatively static and well understood, such as first and last name, title, and job function.

Roles are part of a user's identity and define the user's purpose and responsibilities.

Within identity management, resources define what a user can and does do. In an enterprise, this typically translates into what resources a user has access to, what privileges they have on that resource, and what they have been doing on that resource. Resources can be application accounts or physical devices such as laptops or access cards. The enterprise owns the resources, secures them, and manages access to the resources by managing the user's identity and access.

Relationships establish the portion of user identities that involve organizational transactions such as approvals.

An Oracle Fusion Applications user and corresponding identity are usually created in a single transaction, such as when a worker is created in Human Resources (HR). That transaction automatically triggers provisioning requests for the user based on role provisioning rules.

User accounts for some identities that are not employees, such as partner contacts, may be created in a later transaction using an identity that is already created in the identity store. Supplier contacts are created in the Supplier Model, not HR.

Stores

Various locations store identity and user data.

Identity data consists of the following.

- HR person records

- Oracle Fusion Trading Community Model party records

In Oracle Fusion Applications, identities and users correspond one to one, but not all identities correspond to a user, and not all users are provisioned with an identity. Some identities stored in HR and Trading Community Model may not be provisioned to user accounts and therefore are not synchronized with Oracle Identity Management (OIM). For example, a contact for a prospective customer is an identity in Trading Community Model but may not be provisioned with a user account in OIM. Some users stored in the Lightweight Directory Access Protocol (LDAP) store may not be provisioned with identities. For example, system user accounts used to run Web services to integrate third party services with Oracle Fusion Applications are not associated with a person record in HR or Trading Community Model. Some identifying credentials such as name, department, e-mail address, manager, and location are stored with user data in the LDAP store.

Importing Users

You can import users or user attributes in bulk from existing legacy identity and user stores.

Your tasks may include the following.

- Create users in bulk
- Update specific attributes for all users, such as postal code
- Link users to HR or Trading Community Model persons
- Monitor progress of the import process
- Correct errors & re-import
- Export users in bulk
- Import and export users using a standard plain text data interchange format like Lightweight Data Interchange Format (LDIF)

You can reserve a specific user name not currently in use for use in the future, or release a reserved username from the reservation list and make it available for use. Between a user registration request and approved registration, Oracle Fusion Applications holds the requested user name on the reservation list, and releases the name if an error occurs in the self-registration process or the request is rejected. Self-registration processes check the reservation list for user name availability and suggest alternative names.

Provisioning Events

New identities, such as new hires, trigger user and role provisioning events. In addition to user creation tasks, other tasks, such as Promote Worker or Transfer Worker, result in role provisioning and recalculation based on role provisioning rules.

When an identity's attributes change, you may need to provision the user with different roles. Role assignments may be based on job codes, and a

promotion triggers role provisioning changes. Even if the change in the identities attributes requires no role assignment change, such as with a name change, OIM synchronizes the corresponding user information in the LDAP store.

Deactivating or terminating an identity triggers revocation of some roles to end all assignments, but may provision new roles needed for activities, such as a pay stub review. If the corresponding user for the identity was provisioned with a buyer role, terminating the identity causes the user's buyer record in Procurement to be disabled, just as the record was created when the user was first provisioned with the buyer role.

Notifications and Audits

Oracle Fusion Applications provides mechanisms for notifying and auditing requests or changes affecting identities and users.

Oracle Fusion Applications notifies requestors, approvers, and beneficiaries when a user account or role is provisioned. For example, when an anonymous user registers as a business-to-customer (B2C) user, the B2C user must be notified of the registration activation steps, user account, password and so on once the approver (if applicable) has approved the request and the user is registered in the system.

User ID and GUID attributes are available in Oracle Fusion Applications session information for retrieving authenticated user and identity data.

End user auditing data is stored in database WHO columns and used for the following activities.

- Setting up sign-in audit
- Using the application monitor
- Notifying of unsuccessful sign ins
- Sign-in audit reports

You can conduct real time audits that instantiate a runtime session and impersonate the target user (with the proxy feature) to test what a user has access to under various conditions such as inside or outside firewall and authentication level.

For information on configuring audit policies and the audit store, see the Oracle Fusion Applications Administrator's Guide.

Delegated Administration

You can designate local administrators as delegated administrators to manage a subset of users and roles.

Delegated administrators can be internal or external persons who are provisioned with a role that authorizes them to handle provisioning events for a subset of users and roles.

For example, internal delegated administrators could be designated to manage users and roles at the division or department level. External delegated

administrators could be designated to manage users and roles in an external organization such as a primary supplier contact managing secondary users within that supplier organization.

You can also define delegated administration policies based on roles. You authorize users provisioned with specific roles named in the policy to request a subset of roles for themselves if needed, such as authorizing a subset of roles for a subset of people. For example, the policy permits a manager of an Accounts Payables department to approve a check run administrator role for one of their subordinates, but prohibits the delegated administrator from provisioning a budget approver role to the subordinate.

Credentials

You activate or change credentials on users by managing them in Oracle Identity Management (OIM)

Applications themselves must be credentialed to access one another.

Oracle Fusion Applications distinguishes between user identities and application identities (APPID). Predefined application identities serve to authorize jobs and transactions that require higher privileges than users.

For example, a payroll manager may submit a payroll run. The payroll application may need access to the employee's taxpayer ID to print the payslip. However, the payroll manager is not authorized to view taxpayer IDs in the user interface as they are considered personally identifiable information (PII).

Calling applications use application identities (APPID) to enable the flow of transaction control as it moves across trust boundaries. For example, a user in the Distributed Order Orchestration product may release an order for shipping. The code that runs the Pick Notes is in a different policy store than the code that releases the product for shipment. When the pick note printing program is invoked it is the Oracle Fusion Distributed Order Orchestration Application Development Framework (ADF) that is invoking the program and not the end user.

Provisioning Access: Points To Consider

Various considerations affect how your enterprise provisions access.

You can migrate role memberships, such as from test to production. However, such a bulk Lightweight Directory Access Protocol (LDAP) import sacrifices the automatic control of role assignments that are provided by role provisioning rules when user data changes.

Tip

As a security guideline, maintain role memberships through role provisioning rules. Human Capital Management (HCM) role provisioning rules define what

HR Person or CRM Party criteria are associated with roles. Supplier Portal provisioning rules apply to users provisioned through the Supplier application.

When upgrading to a new release of Oracle Fusion Applications, you only need to migrate users and users' role memberships if the LDAP server changes..

Access provisioning task flows are either administered or self service. Administered provisioning requires you to initiate requests and manage users on behalf of users and the enterprise. In self service provisioning, users initiate the provision requests.

Administered Access

Provision to users only those job roles that are not inherited by data roles you could provision instead.

Tip

As a security guideline, provision the data roles that grant access to a specific set of instances within a business object, based on the user being provisioned.

For example, when provisioning the Accounts Payables Manager job role to a user in the US business unit, you select the Accounts Payables Manager US data role, which grants access to person, payroll, location, and position in that dimension.

Self Service Access

Self service access provisioning in Oracle Fusion Applications generates approval requests. You may configure provisioning requests to be automatically approved for certain roles. For example, when a line manager requests roles on behalf of a new hire.

Oracle Identity Management (OIM) supports self registration flows where users expect access as soon as the registration is complete. If the user has not been registered or the required roles have not been provisioned to the user, the self registration attempt triggers a role provisioning request.

Oracle Fusion Applications supports image-based authentication in self-registration scenarios.

Request Management

Duty roles cannot be requested and should not be provisioned on a role request. Role requests adhere to segregation of duties policies.

Passwords are stored in Oracle Identity Management (OIM) based on OIM password policies.

For information about configuring user attributes and password policies, see the Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager

Role Provisioning and Segregation of Duties: How They Work Together

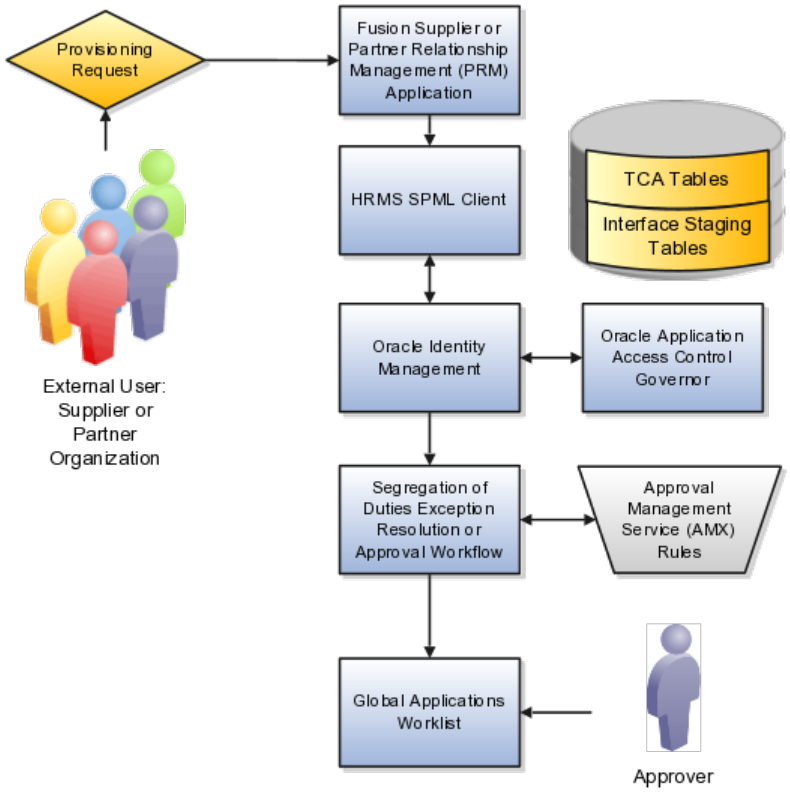
Segregation of duties (SOD) checks occur when roles are assigned to users. The checks are based on Oracle Application Access Controls Governor (AACG) policies in Oracle Enterprise Governance, Risk and Compliance (GRC). The Oracle Identity Management (OIM) integration includes predefined routing rules for remediation in the Manage IT Security business process.

External users such as suppliers or partners need to be provisioned with roles to facilitate access to parent company interfaces and data. The process by which such provisioning requests are approved in Oracle Fusion Applications helps explain the request flows and possible outcomes.

Note

In Oracle Identity Management (OIM), external users means users who are not specific to applications, such as enterprise roles or the absence of entitlement to access an application.

The figure shows the role provisioning request flow. OIM uses AACG to check segregation of duties violations.



Tables

A supplier or partner requests admission to a program using an implementation of the Supplier Portal Submission. The submission is captured in one or both of the following tables in advance of approving or rejecting the supplier or partner.

- Oracle Fusion Trading Community Model
- Interface Staging

Oracle Fusion Applications collects the employee names for the supplier or partner company at the time the company submits its request to join the program so that all employees accessing Oracle Fusion Applications on behalf of the supplier or partner are provisioned.

AACG in the Oracle Enterprise Governance, Risk and Compliance (GRC) suite is certified to synchronize with the policy and identity stores for all pillars or partitions of Oracle Fusion Applications and integrated with the Oracle Fusion Applications security approach to roll up entitlements (by means of duty roles) to the roles that are provisioned to internal users. SOD policies can be defined and enforced at any level of authorization. For external users, SOD policies use attribute information stored in the Trading Community Model tables.

OIM and the SPML Client

Enterprise business logic may qualify the requester and initiate a role provisioning request by invoking the Services Provisioning Markup Language (SPML) client module, as may occur during onboarding of internal users with Human Capital Management (HCM), in which case the SPML client submits an asynchronous SPML call to OIM. Or OIM handles the role request by presenting roles for selection based on associated policies.

OIM recognizes the role provisioning request and initiates a call to AACG.

OIM apprises the SPML client of the current state of the role provisioning request as SOD_CHECK_IN_PROGRESS.

OIM stores the SOD check result as part of OIM audit data.

OIM apprises SPML client of the current state of the SPML request. The provisioning is either still in progress with segregation of duties being checked, or conflicts were found. If conflicts exist, AACG rejects the request and notifies the application.

Status	Conflicts	Current State
SOD_CHECK_IN_PROGRESS	Unknown	Request sent to AACG and waiting for response
SOD_REMEDIATION_IN_PROGRI	Conflict found	AACG detected violations and remediation is in progress
SOD_CHECK_APPROVED	No conflict found	No SOD violations found
SOD_CHECK_REJECTED	Conflict found	AACG detected violations that cannot be remediated
SOD_REMEDIATION_APPROVED	Conflict found	AACG detected violations that are approved

SOD_REMEDIATION_REJECTED	Conflict found	AACG detected violations that are rejected by approver

In the absence of an SOD exception, OIM provisions all relevant users.

Note

When a partner user is provisioned, all employees of the partner enterprise are provisioned. SOD checks occur when an external user requests to join a program, because SOD policies operate across Oracle Fusion Applications, not at the individual level. Supplier or partner company user requests are not approved if there is an SOD conflict against the supplier company.

OIM provides AACG with the details of SOD exception approval workflow. AACG audits the outcome for use in future detective controls and audit processes.

Oracle Application Access Controls Governor

AACG may respond with the following.

- Roles may be provisioned to the external user or its employees because no SOD conflict is found
- SOD conflict is found and request is denied because the relevant SOD policy is to be strictly enforced and no exception approval should be allowed
- SOD conflict is found and the exception to the policy is allowed, so the request goes through additional processing, such as an approval process.

Supplier or Partner Relationship Management responds to an SOD exception by updating Trading Community Model tables with the current state. An enterprise may elect to implement a landing pad that offers external users a means of addressing the SOD problem by providing more information or withdrawing the request.

SOD violation checking occurs during role implementation and provisioning, and can be turned on or off if AACG is provisioned and enabled as part of the Oracle Fusion Applications deployment.

Segregation of Duties Exception Resolution or Approval Workflow

Depending upon status, OIM kicks off an auditable SOD exception resolution workflow. Resolution can be conditional based on approval or requirements such as contracts being met.

If one of the paths for exception resolution is to get an approval, then the SOD exception resolution drives the approval using AMX. Standard AMX rules, not business rules, resolve the approval for the SOD exception, including the following.

- Organizational hierarchies
- Multiple mandatory and optional approvers

- Rerouting and approval delegation

The approver resolution uses AMX Rules Designer to access various user attributes and organizational hierarchies managed in Oracle Fusion Applications repositories. This information is typically not available in OIM or the LDAP identity store repository. Enterprises can define additional approval rules using AMX Thin Client.

The SOD Exception Approver gets a notification through supported channels that a new request is awaiting approval. The approver signs in to the global SOA federated worklist application that aggregates all pending worklist items for the user from all Oracle Fusion applications and logical partitions or pillars of applications. The SOD exception approval tasks show up in the same list.

The SOD exception approval task shows the details of the SPML request and SOD Provisioning results in a page rendered by OIM. The approver may take one of the following actions.

- Approve the request as it is
- Reject the request

If the approver approves the request, OIM sends an SOD_REMEDIATION_APPROVED status to the SPML client.

If the approver rejects the request, OIM sends an SOD_REMEDIATION_REJECTED status to the SPML client. The provisioning request is considered completed with a failure outcome and the external users is notified. Oracle Fusion Applications updates the Trading Community Model tables with the rejected status

Remediation Task Assignments

The SOD remediation tasks are assigned based on the role being requested.

1. If the role requested is Chief Financial Officer, the SOD remediation task is assigned to the IT Security Manager role.
2. If the SOD violation results from a policy where the SOD control tag is the Information Technology Management business process and the control priority is 1, the SOD remediation task is assigned to Application Administrator role.
3. In all other scenarios, the SOD remediation task is assigned to the Controller role.

For more information about configuring audit policies, see the Oracle Fusion Applications Administrator's Guide.

For information on managing segregation of duties, see the Oracle Application Access Controls Governor Implementation Guide and Oracle Application Access Controls Governor User's Guide.

11

Security Reference Implementation

Scope of the Security Reference Implementation: Explained

The Oracle Fusion Applications security reference implementation consists of predefined business processes, roles, role memberships, entitlement, and policies.

The security reference implementation includes the following.

- A business process model (BPM)
- Predefined data
- Security policies
- Security rules
- Security implementation life cycle

The security reference implementation in Fusion Applications provides a predefined security implementation that is applicable to the needs of midsized (generally between 250 and 10,000 employees), horizontal enterprises and can be changed or scaled to accommodate expansion into vertical industries such as health care, insurance, automobiles, or food manufacturing.

Predefined Data

The security reference implementation associates a full range of predefined roles with the business process model (BPM) levels. When assigned to users, the enterprise roles guide and control access to the task flows of the BPM and associated data. At the task level, task flows define the business actions that fulfill the intent of the BPM.

A security reference manual (SRM) for each offering presents all predefined roles, role hierarchies, business objects the roles must access, segregation of duties policies, and jobs that may have conflicting duties according to those policies. The reference implementation also can be viewed using the integrated Authorization Policy Manager (APM) and Oracle Identity Management (OIM) user interface pages to manage security policies, users, and identities.

Business Process

The Oracle Fusion Applications security reference implementation provides predefined roles assigned to a business process model of activities and tasks.

For example, the IT Security Manager role is assigned to the Manage Job Roles task in the Implement Function Security Controls activity, which belongs to the Manage IT Security detailed business process of the Information Technology Management business process. In Oracle Fusion Applications, you perform the Manage Job Roles task using Oracle Identity Management (OIM).

Security Policies

The Oracle Fusion Applications security reference implementation provides predefined policies for data security, function security, segregation of duties, and implementation life cycle management. An enterprise sets policies for authorization, authentication, and privacy.

The predefined security policies of the security reference implementation form the foundation of Oracle Fusion Applications security and can be inspected and confirmed to be suitable or the basis for further implementation with the Application Authorization Policy Manager.

Predefined segregation of duties policies prevent errors and fraud caused by giving a user control over two or more phases of secured business transactions or operations, such as custody, authorization or approval, and recording or reporting of related transactions affecting an asset.

Predefined information life cycle management policies secure data from live database, through backup, archive, and purge.

Predefined authorization policies are the function and data security of the security reference implementation. The policies define permissions for an entity to perform some action, such as view, update, or personalize, against some resource, such as a task flow. The permissions are grouped as privileges, which comprise the entitlement granted to duty roles. Access Control Rule and grants of entitlement together identify the actions allowed on an entity by a resource.

Authentication policies certify the trustworthiness of an identity. Oracle Identity Management (OIM) stores passwords in encrypted form in Lightweight Directory Access Protocol (LDAP). OIM can delegate authentication to Oracle Access Manager.

Predefined privacy policies protect sensitive information about an identity.

Other Rules That Affect the Security Reference Implementation

The security reference implementation does not include predefined provisioning rules or auditing rules.

In Oracle Fusion General Ledger, accounting flexfield segment security rules secure balancing segment values.

Security Implementation Life Cycle

At a high level, the security implementation life cycle follows the same phases as other aspects of information technology.

A planning phase allows for understanding the security requirements of your enterprise and mapping those to Oracle Fusion Applications security as reflected in the reference implementation. The implementation phase fulfills those requirements and a deployment phase puts your Oracle Fusion Applications implementation into secured production with your users, customers, and

partners. The maintenance phase addresses security upgrades and modifications as your enterprise and Oracle Fusion Applications evolve.

Patches to the security reference implementation preserve your changes to the implementation. Patching the security reference implementation preserves enterprise security changes of the reference implementation because your enterprise' security implementation is a copy of the reference implementation with changes.

Role Types in the Security Reference Implementation: Explained

Oracle Fusion Applications security provides four types of roles: abstract, job, duty, and data.

The reference implementation contains predefined abstract, job, and duty roles in hierarchies that streamline provisioning access to users.

- Abstract roles
- Job roles
- Duty roles
- Data roles
- Role hierarchies

For example, a worker may be provisioned with the Employee abstract role. In addition, the worker may be an accounts payable manager for the US business unit. Since the reference implementation provides for a data role to be generated based on the Financials Common Module Template for Business Unit Security role template, the worker is also provisioned with the Accounts Payable Manager - US data role. That data role inherits the Accounts Payables Manager job role in a role hierarchy, which includes descendent duty roles that an accounts payable manager requires to perform the duties of the job.

Note

Abstract, job, and data roles are enterprise roles in Oracle Fusion Applications. Oracle Fusion Middleware products such as Oracle Identity Manager (OIM) and Authorization Policy Manager (APM) refer to enterprise roles as external roles. Duty roles are implemented as application roles in APM and scoped to individual Oracle Fusion Applications.

Abstract Roles in the Reference Implementation

An abstract role is a type of enterprise role that is not specific to a particular job.. The reference implementation contains predefined abstract roles, such as Employee or Contingent Worker.

Abstract roles inherit duty roles as a means of accessing application functions and data that users require to perform the tasks associated with the duties of work not specific to a particular job.

Provision abstract roles directly to users.

Some Oracle Business Intelligence Foundation Suite for Oracle Applications (OBIFA) abstract roles provide the job roles that inherit them with access to reports and analytics.

Job Roles in the Reference Implementation

Job roles are a type of enterprise role, called an external role in OIM and APM. The reference implementation contains predefined job roles.

Job roles inherit duty roles as a means of accessing application functions that users require to perform the tasks associated with the duties of the job. Job roles are not assigned entitlement to access functions directly. You change job roles by changing their hierarchy of inherited abstract and duty roles. Job roles may inherit other job roles, abstract roles, and duty roles.

The job roles in the reference implementation grant no explicit access to data. To grant access to specific data for a job role, you can define a data role.

You can provision job roles directly to users, and would do so if no data roles are available that inherit the job role. Job roles may grant access to data implicitly through data security policies defined for the duty roles that the job role inherits.

Important

As a security guideline, if data roles are associated with a job role, provision the data role to the user instead of the job role.

Duty Roles in the Reference Implementation

Duty roles are a type of application role. The reference implementation contains predefined duty roles. For example, the Accounts Payable Manager job role inherits the Approving Payables Invoices Duty role. For example, the Human Resource Specialist job role inherits the Worker Administration Duty role.

Duty roles provide access to the application functions that users require to perform the tasks associated with the duty. The access is defined as entitlement, which consist of privileges.

Duty roles are the building blocks of role based access control and cannot be changed. For reasons of security life cycle management, Oracle Fusion Applications implementations should use the predefined duty roles and not add custom duty roles unless you are adding custom application functions that require a new or modified duty role.

All predefined duty roles respect the segregation of duties constraints defined in the reference implementation.

Note

Duties or tasks carried by Oracle Fusion Applications enterprise roles may be incompatible according to the segregation of duties policies of the reference implementation, but any single duty role is free from an inherent segregation of duties violation.

Data Roles in the Reference Implementation

Data roles are a type of enterprise role, called an external role in OIM and APM. The reference implementation does not contain predefined data roles. Data roles are specific to an enterprise. Data role templates in the reference implementation provide predefined structures for defining data roles.

The data roles that product family implementation users define for the enterprise carry explicit data access grants and may inherit abstract, duty or job roles.

Provisioning a user with a data role augments the inherited abstract, duty or job roles with entitlement to access data. The access is explicit because the grant is defined based on the needs and data of the enterprise. For example, Accounts Payable Manager - US Business Unit data role is given explicit access to the US accounts payable data and inherits the job role Accounts Payable Manager. US Business Unit represents data determined by your enterprise and is not part of the Oracle Fusion reference implementation.

Provision data roles directly to users. As a security guideline, provision a data role, rather than also provisioning a job role that the data role inherits.

Data roles can be defined as a hierarchy of data roles.

Role Hierarchies in the Reference Implementation

Role hierarchies are structured to reflect your enterprise.

Job roles inherit duty roles. For example, the Accounts Payable Specialist job role inherits the Invoice Reviewer Duty and Invoice Receiver Duty roles.

Job roles can inherit one or more other job roles. For example, the Chief Financial Officer job role inherits the Controller job role, and the Applications Implementation Consultant role inherits the Application Administrator roles of the product families, such as the Human Capital Management Application Administrator job role required for core HCM setup.

Job roles can inherit abstract roles, such as the Accounts Payable Specialist and Accounts Payable Manager job roles inheriting the Employee abstract role, and a Warehouse Manager inheriting the Contingent Worker abstract role.

Important

To give enterprises the flexibility to decide if, for example, a job role is filled by employees or contingent workers, the reference implementation contains no predefined role hierarchies in which a job role inherits an abstract role.

Most job roles do not grant access to data. To provide data access for such job roles, you must generate data roles using the data role templates provided by the reference implementation. The data roles you generate inherit the base job role.

Abstract roles can inherit one or more other abstract roles. The Employee abstract role inherits the Procurement Requester abstract role.

Abstract roles can inherit one or more other duty roles. The Employee role inherits the Worker Duty role.

Abstract roles make use of implicit data security and generally are not inherited by data roles. For example, user context determines which data the Employee abstract role can access.

The predefined roles and role hierarchies are listed in the Oracle Fusion Applications Security Reference Manual for each offering.

Function Security in the Security Reference Implementation: Explained

In the security reference implementation, function security policies entitle a role to access a function in Oracle Fusion Applications unconditionally.

Predefined function security consists of roles and security policies. Details of the security reference implementation can be viewed in security reference manuals (SRM) for each offering and in the Authorization Policy Management.

Functions are secured with the following standard approaches.

- Role-based access control
  - Set of job roles
  - Duty roles and role hierarchy for each job and abstract role
  - Access entitlement granted to each duty role
- Segregation of duties policies

If the roles of your enterprise fall outside the scope of the security reference implementation, you may need to extend your Oracle Fusion Applications and predefined function security with new job and duty roles.

Function Access Based on Job and Duty Roles

The duties that define jobs consist of access to those application functions that are used to perform the duty.

Predefined function security policies give grants of entitlement to access functions for the purpose of carrying out the actions associated with a duty. Duties are segregated to prevent combining grants in a duty role that should be separated across multiple roles, such as approving, recording, processing, and reconciling results.

Extending the Function Security of the Reference Implementation

The predefined security reference implementation is a general case representing security guidelines. Your enterprise may require additional roles with specific constraints on accessing application functions.

For example, your enterprise is a bank with a bank manager job role. Create this new job role as a new group in the Lightweight Directory Access Protocol (LDAP) identity store by performing the Manage Job Roles or Create Job Roles tasks in Oracle Identity Management (OIM). Define the job role to inherit the duties of a bank manager, as defined by the available predefined duty roles. Create the role hierarchy of duty roles for the new job role using the Manage Duties task in Authorization Policy Manager (APM)..

If your enterprise is a pharmaceutical company, you may have users who must perform clinical trial administration duties. If the applications that a user must access to administer a clinical trial are already part of Oracle Fusion Applications, a new duty can be created in Authorization Policy Manager with entitlement to the resource code or functions users need to access for performing clinical trial administration duties. The new duty role is then associated with an enterprise role, which is represented by a group in LDAP and thereby made available for provisioning to users.

The security reference implementation can be viewed in the user interfaces where security tasks are performed or in the security reference implementation manual (SRM) for each Oracle Fusion Applications offering.

Data Security in the Security Reference Implementation: Explained

The reference implementation contains a set of data security policies that can be inspected and confirmed to be suitable or a basis for further implementation using the Authorization Policy Manager (APM).

The security implementation of an enterprise is likely a subset of the reference implementation, with the enterprise specifics of duty roles, data security policies, and HCM security profiles provided by the enterprise.

The business objects registered as secure in the reference implementation are database tables and views.

Granting or revoking object entitlement to a particular user or group of users on an object instance or set of instances extends the base Oracle Fusion Applications security reference implementation without requiring customization of the applications that access the data.

Data Security Policies in the Security Reference Implementation

The data security policies in the reference implementation entitle the grantee (a role) to access instance sets of data based on SQL predicates in a WHERE clause.

Tip

When extending the reference implementation with additional data security policies, identify instance sets of data representing the business objects that need to be secured, rather than specific instances or all instances of the business objects.

Predefined data security policies are stored in the data security policy store, managed in the Authorization Policy Manager (APM), and described in the Oracle Fusion Applications Security Reference Manual for each offering. A data security policy for a duty role describes an entitlement granted to any job role that includes that duty role.

Warning

Review but do not modify HCM data security policies in APM except as a custom implementation. Use the HCM Manage Data Role And Security Profiles task to generate the necessary data security policies and data roles.

The reference implementation only enforces a portion of the data security policies in business intelligence that is considered most critical to risk management without negatively affecting performance. For performance reasons it is not practical to secure every level in every dimension. Your enterprise may have a different risk tolerance than assumed by the security reference implementation.

HCM Security Profiles in the Security Reference Implementation

The security reference implementation includes some predefined HCM security profiles for initial usability. For example, a predefined HCM security profile allows line managers to see the people that report to them.

The IT security manager uses HCM security profiles to define the sets of HCM data that can be accessed by the roles that are provisioned to users

Data Roles

The security reference implementation includes no predefined data roles to ensure a fully secured initial Oracle Fusion Applications environment.

The security reference implementation includes data role templates that you can use to generate a set of data roles with entitlement to perform predefined business functions within data dimensions such as business unit. Oracle Fusion Payables invoicing and expense management are examples of predefined business functions. Accounts Payable Manager - US is a data role you might generate from a predefined data role template for payables invoicing if you set up a business unit called US.

HCM provides a mechanism for generating HCM related data roles.

Segregation of Duties in the Security Reference Implementation: Explained

Segregation of duties (SOD) is a special case of function security enforcement. A segregation of duties conflict occurs when a single user is provisioned with a role or role hierarchy that authorizes transactions or operations resulting in the possibility of intentional or inadvertent fraud.

The predefined SOD policies result in duty separation with no inherent violations. For example, an SOD policy prevents a user from entitlement to create both payables invoices and payables payments.

However, the most common duties associated with some job and abstract roles could conflict with the predefined segregation of duties. A predefined role hierarchy or job or abstract role may include such common duties that are incompatible according to a segregation of duties policy. For example, the predefined Accounts Payable Supervisor job role includes the incompatible duties: Payables Invoice Creation Duty and Payables Payment Creation Duty.

Every single predefined duty role is free from an inherent segregation of duties violation. For example, no duty role violates the SOD policy that prevents a user from entitlement to both create payables invoices and payables payments.

Jobs in the reference implementation may contain violations against the implemented policies and require intervention depending on your risk tolerance, even if you define no additional jobs or SOD policies.

Provisioning enforces segregation of duties policies. For example, provisioning a role to a user that inherits a duty role with entitlement to create payables invoices enforces the segregation of duties policy applied to that duty role and ensures the user is not also entitled to create a payables payment. When a role inherits several duty rules that together introduce a conflict, the role is provisioned with a violation being raised in the Application Access Controls Governor (AACG). If two roles are provisioned to a user and introduce a segregation of duties violation, the violation is raised in AACG.

Note

SOD policies are not enforced at the time of role definition.

Aspects of segregation of duties policies in the security reference implementation involve the following.

- Application Access Controls Governor (AACG)
- Conflicts defined in segregation of duties policies
- Violations of the conflicts defined in segregation of duties policies

Application Access Controls Governor (AACG)

AACG is a component of the Oracle Enterprise Governance, Risk and Compliance (GRC) suite of products where segregation of duties policies are defined.

- Define SOD controls at any level of access such as in the definition of an entitlement or role.
- Simulate what-if SOD scenarios to understand the effect of proposed SOD control changes.
- Use the library of built-in SOD controls provided as a security guideline.

Your risk tolerance determines how many duties to segregate. The greater the segregation, the greater the cost to the enterprise in complexity at implementation and during maintenance. Balance the cost of segregation with the reduction of risk based on your business needs.

Conflicts

An intra-role conflict occurs when a segregation of duties policy expresses constraints within the construct of a single role (entitlement and duties) that creates violations.

Tip

As a security guideline, use only the predefined duty roles, unless you have added new applications functions. The predefined duty roles fully represent the functions and data that must be accessed by application users and contain all appropriate entitlement. The predefined duty roles are inherently without segregation of duty violations of the constraints used by the Application Access Controls Governor.

Violations

A segregation of duties violation occurs when a policy is defined that allows a segregation of duties conflict to occur.

Notifications report conflicts to the requester of the transaction that raised the violation. Oracle Identity Management (OIM) shows the status of role requests indicating if a segregation of duties violation has occurred.

For information on configuring audit policies, see the Oracle Fusion Applications Administrator's Guide.

For more information on managing segregation of duties, see the Oracle Application Access Controls Governor Implementation Guide and Oracle Application Access Controls Governor User's Guide.

Extending the Security Reference Implementation: Critical Choices

In general, the security reference implementation is designed to require only small deltas to adjust the Oracle Fusion Applications security approach for a specific enterprise.

Most commonly, the security reference implementation is extended with the following.

Common Extension	Reasons
New job with existing duties	Create a new job role and map existing duty roles to it, if the job titles in your enterprise do not match the job titles in the security reference implementation, but the job's duties are performed by people with different job titles.
Existing duty with different existing entitlement	Change the existing entitlement grants of an existing duty role to reflect the access required to all tasks that need to be performed by that duty at your enterprise.
New duty with existing entitlement	Create a new duty role with existing entitlement for duties that are not available with that entitlement in the security reference implementation, but that are required by the job roles in your enterprise.
New hierarchy with existing duties	Create new hierarchies of existing duties to reflect the access required by the job roles in your enterprise.
New job with new duties	Create new job roles and new duty roles for providing access to custom applications.

Every feature in a Oracle Fusion Application deployment corresponds to one or more duty roles predefined to use the feature. When your enterprise does not use every feature, it does not need to provision every predefined duty role.

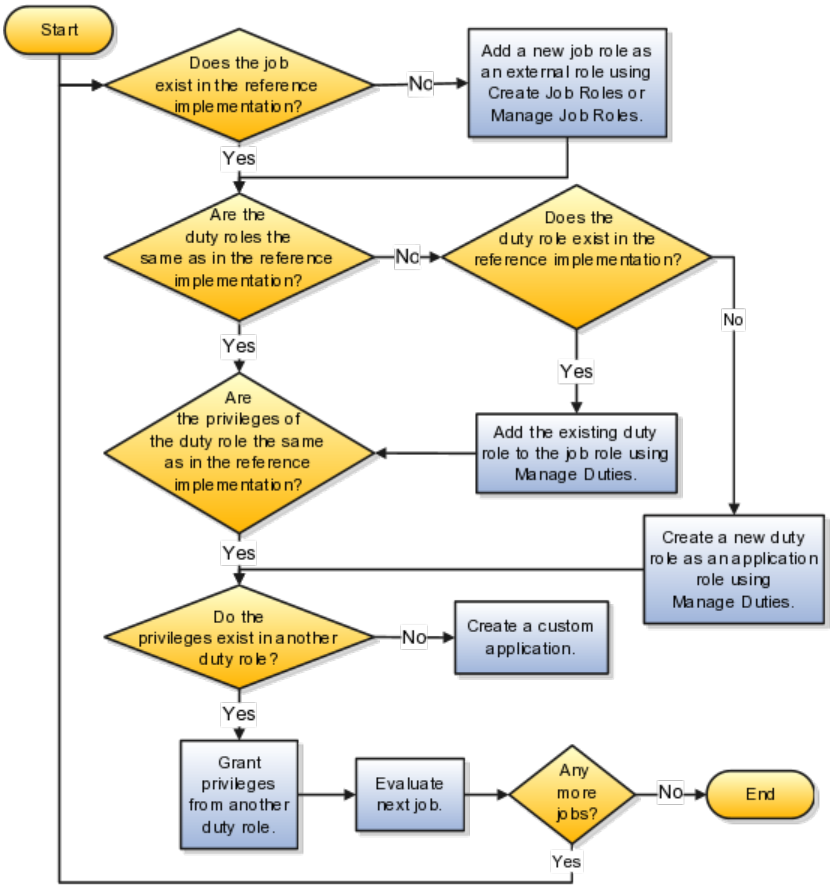
Assess the security reference implementation during planning. The security reference implementation can be viewed in the user interfaces where security tasks are performed or in the security reference manual (SRM) for each Oracle Fusion Applications offering.

Types of Changes

The common decisions made to match an enterprise to the security reference implementation include the following:

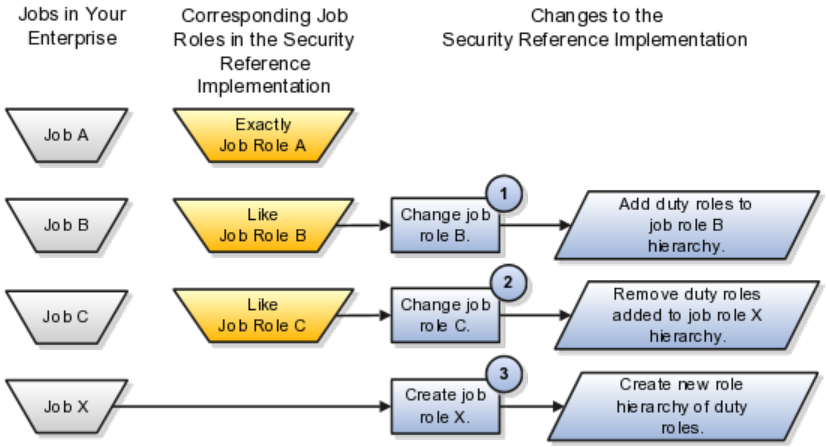
- Do the predefined job roles match the equivalent job roles in your enterprise?
- Do the jobs in your enterprise exist in the security reference implementation?
- Do the duties performed by the jobs in your enterprise match the duties in the security reference implementation?

In the figure, various tasks correspond to the decisions you make about changing the security reference implementation.



The following figure shows some examples of changes that may be required to match the security reference implementation job roles to the job roles of your enterprise.

1. Add duty roles to a predefined job role hierarchy.
2. Remove duty roles from a predefined job role hierarchy to include as a new, separate job role.
3. Create a new job role with a hierarchy of predefined duty roles, some of which may be duty roles you removed from a predefined job role hierarchy.



All functions and actions in Oracle Fusion Applications that need to be secured are covered by the reference implementation. In some cases, especially with function customizations, a new duty role may be needed.

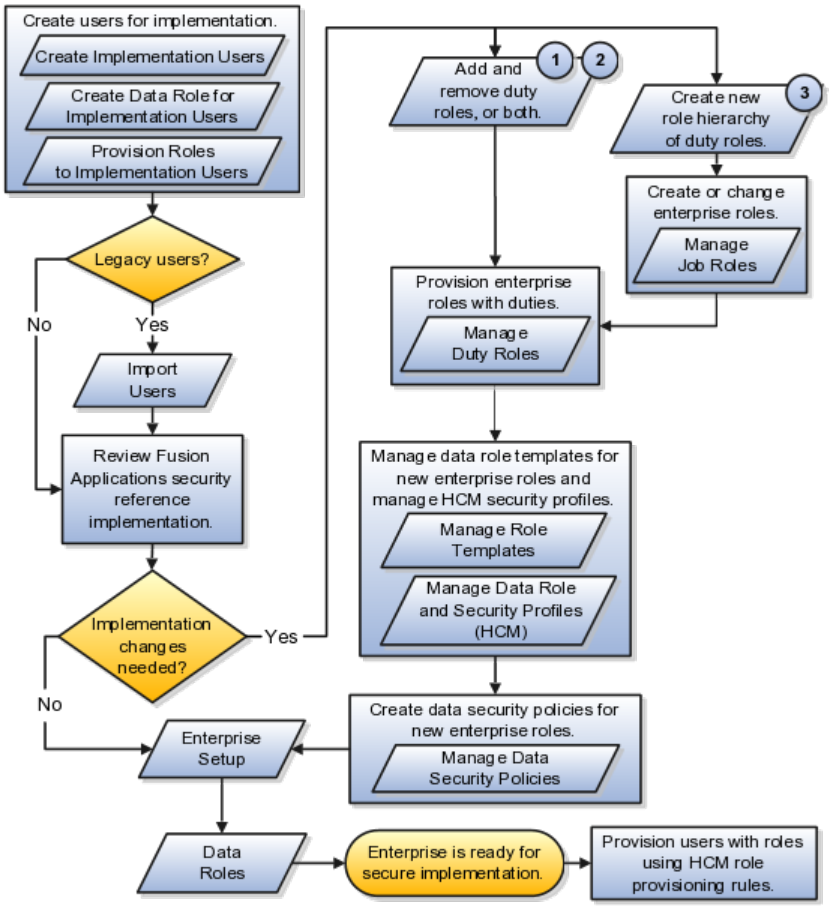
Changes to data security require changing data security policies and the data roles templates.

For information on securing new business objects in Customer Relationship Management (CRM) Application Composer and securing new business objects in an extended application, see the Oracle Fusion Applications Extensibility Guide.

Implementation Flow

The security implementation flow ranges from creating users for implementation to provisioning users with roles so they can implement the deployment for their enterprise. Most of the tasks in the flow after creating users for implementations and before setting up the enterprise are optional. In particular, you only need to manage data role templates and data security policies if you have data security needs not addressed by the security reference implementation.

The following figure shows the Oracle Fusion Applications security implementation flow with the three examples of changes made to extend a security reference implementation.



Note

Use one of two ways to create data roles

- Generate data roles by using data role templates, which secure data based on enterprise setup of data dimensions such as business unit.
- Create HCM security profiles, which define data security conditions on instances of object types such as person records, positions, and document types.

FAQs for Security Reference Implementation

What's an entitlement?

An action that is conditionally or unconditionally granted to a user or role to access functions and data. In most contexts, entitlement is equivalent to privilege.

Entitlement provides the means necessary to access or act upon business objects, including Oracle Business Intelligence Foundation Suite for Oracle Applications (OBIFA) objects. There is a one-to-one mapping between an operation and entitlement. For example, the Create Purchase Order operation is granted as a privilege to a role with entitlement to approve a purchase order.

In function security, entitlement is a set of privileges. Each privilege enables a single action, such as Enter Payable Invoice. A single action consists of permissions on the resources relevant to the action.

In data security, entitlement is conditionally granted to a role on a named set of data. For example, a Payables Accountant is entitled to delete an invoice with invoice_id=100. The entitlement includes the privilege that allows the accountant to read this invoice with the delete function enabled.

An Oracle Enterprise Governance, Risk and Compliance (GRC) entitlement is a set of permissions defined in the Oracle Application Access Controls Governor (AACG) to participate in segregation of duties policies.

12

Enforcement Across the Information Life Cycle

Secure Information Life Cycle: Explained

The information life cycle of a business is the movement of products and data from beginning to end through the following stages.

- Installation
- Implementation
- Test
- Production and change control
- Archive or back up
- Purge

Oracle Fusion Applications data security policies are applicable and active at each stage.

Oracle Fusion Applications optionally respects the Information Life Cycle Management policies that your enterprise establishes based on business goals and drivers. These policies likely adhere to the following.

- Overall IT governance and management
- Change control processes
- Requirements for system availability and recovery times
- Service level agreements (SLAs)

Oracle Fusion Applications provides encryption application programming interfaces (APIs) to protect sensitive fields in application user interfaces. Oracle Fusion Applications is certified to use the Oracle Advanced Security option for the Oracle database. Oracle Fusion Applications deploys with features of this option, such as Transparent Data Encryption (TDE) and Oracle Database Vault (ODV), enabled if installed. TDE and ODV provide information life cycle protections such as the following.

- Data access restrictions on database administrators and other privileged users
- Sensitive data at rest in database files and file backups
- Sensitive data in transit
- Sensitive attributes in non-production databases

With these protections, database administrators do not have access rights to select from tables in applications that they administer. Oracle Fusion encrypts sensitive data as it is written to file, either on disk or in backup. Network security protects sensitive data in transit. Sensitive data is masked when you create test databases from production databases.

Access Restrictions on Entitled Users

Oracle Database Vault (ODV) establishes limitations on the power of entitled users to access sensitive data through segregation of duties policies on database administrator (DBA) roles and by securely consolidating application data in the database.

These limitations prevent DBAs and other privileged users from overriding the protections placed on sensitive data by the Virtual Private Database (VPD). Oracle Fusion Applications deploy with ODV enabled when ODV is installed.

Oracle Database Vault remains enabled during patching.

A single realm protects Oracle Fusion Applications data. DBA's do not have select privileges within the realm within which the applications data resides. You can extend that realm to include integrations with applications that are not Oracle Fusion applications. You can establish subset realms within the Oracle Fusion Applications realm. Adding realms to your Oracle Fusion Applications deployment is a custom implementation.

Transparent Data Encryption

Transparent Data Encryption (TDE) protects confidential data, such as credit card and social security numbers.

Database users need not take any action to decrypt the data when accessed. Decryption is transparent. To prevent unauthorized decryption, transparent data encryption stores the encryption keys in a security module external to the database.

TDE does not require administrators to manage key storage or create auxiliary tables, views, and triggers. You control encryption policies in the Advance Security Option of the Oracle Database.

For more information on TDE, see the Oracle Database Advanced Security Administrator's Guide.

Types of Sensitive Data: Explained

Sensitive data is any data that should not be accessed by everyone or without restriction.

Information lifecycle context and business justifications determine what data is sensitive. Oracle Fusion Applications security protects types of sensitive data variously, depending on access circumstances.

Note

Oracle Fusion Applications encryption application programming interfaces (APIs) mask data such as credit card numbers in application user interface fields. For encryption and masking beyond that, Transparent Data Encryption (TDE) and Oracle Database Vault are certified but optional with Oracle Fusion Applications.

Type of Data	Life Cycle Phase	Protection provided by:	Tool
Oracle Fusion Application data	All	Access restrictions and segregation of duties	Oracle Database Vault, single realm
Sensitive	Installation	Transparent data encryption	Oracle Advanced Security (OAS) and Transparent Data Encryption (TDE)
	Implementation	Transparent data encryption	OAS and TDE
	Test	Data Masking	Oracle Data Masking
	Production and change control	Transparent data encryption	OAS and TDE
	Archive and purge	Transparent data encryption	OAS and TDE
	Data at rest	Transparent data encryption	OAS and TDE
	Data in transit	Network encryption	Network Data Encryption and Data Integrity features of Oracle Advanced Security

Oracle Fusion Applications deploy with Transparent Data Encryption enabled at the tablespace level. Information on disc is encrypted and is transparently decrypted by the database server process.

Oracle Fusion Applications deploy with a Data Masking Pack in Oracle Enterprise Manager allowing clones of the production database to be created with sensitive data masked.

Sensitive Data At Rest

Transparent Data Encryption (TDE) protect sensitive data at rest.

Sensitive Data In Transit

Network Data Encryption and Data Integrity features of Oracle Database Advanced Security protect sensitive data when it is transmitted over the network.

Sensitive Data in Custom Fields

You can use Oracle Data Finder to discover sensitive information in custom fields.

Sensitive Data in Non-production Databases

Data masking removes sensitive data from non-production copies of the database such as when leaving a production environment to conduct testing or when outsourcing, off-shoring, or sharing data with partners.

Note

Regulations such as HIPAA (the Health Insurance Portability and Accountability Act) in the US, and the Data Protection Directive in the European Union mandate the protection of sensitive data.

Oracle Data Masking replaces the sensitive data with randomly generated meaningless data to preserve the integrity of the applications that refer to the data. Once removed, the data cannot be recovered in the non-production copies of the database.

Oracle Fusion Applications use an extensible library of templates and policies to automate the data masking process when you create a clone of your production database. The templates change personal and sensitive data, but preserve the accuracy of enough data to support realistic testing. Validation, formatting, and syntax rules, such as Vertex requirements for a valid combination of city, state and zip code, limit the level of data masking to levels of destruction that preserve realistic testing but are therefore less protective. For example meaningful payroll or tax tests may require addresses to remain unmasked at the state level.

Manage masking definitions using Oracle Enterprise Manager. A masking definition identifies the mask format for the sensitive data and the schema, table, and column of the sensitive attributes. The masking format can be set to generate realistic and fully functional data in place of sensitive data depending on your security requirements and the usage of the cloned database.

For information on viewing data masking definitions, see the Oracle Fusion Applications Administrator's Guide.

For more information on TDE, see the Oracle Database Advanced Security Administrator's Guide.

For information on settings and deployment options to protect sensitive data, see the Oracle Fusion Applications Security Hardening Guide.

For information on settings and deployment options to protect sensitive data, see the Oracle Fusion Applications Security Hardening Guide.

Protecting Sensitive Data: Points To Consider

Sensitive attributes include personally identifiable information(PII) and non-PII attributes.

As a security guideline, consider protecting copies of the sensitive data, as well as the live system.

Oracle Transparent Data Encryption (TDE) prevents access to PII in the file system or on backups or disk. Oracle Virtual Private Database (VPD) protects PII from users with DBA access, and Oracle Data Vault (ODV), if installed, prevents this protection from being overridden. Oracle Data Masking protects PII and sensitive data in cloned databases.

Encryption APIs

Oracle Fusion Applications uses encryption application programming interfaces (APIs) to mask sensitive fields in application user interfaces such as replacing all but the last four digits of a credit card with a meaningless character.

Data Masking Templates

Oracle Data Masking is available for masking data in non-production instances or clones.

Oracle Fusion Applications optionally provides predefined data masking templates as a starting point for use with the Oracle Enterprise Manager Data Masking Pack. The templates specify the tables and columns being masked and the masking formats. Determine the needs of your enterprise or the purpose of database clones and make modifications accordingly by adding or removing the tables and columns being masked, and changing masking formats.

Oracle Enterprise Manager provides views of masked tables and columns.

Warning

Oracle Data Masking converts non production data irreversibly. For example, you can mask data in formats that allow applications to function without error, but the data cannot be reconstituted.

Non-production phases require realistic data, which potentially precludes masking all sensitive data.

Tip

Offset the danger of gaps in masking with business processes that limit unauthorized view of sensitive data. For example, apply the same policies for

handling Human Resources (HR) data to testers as are applied to Human Capital Management (HCM) staff. Provide individual test accounts provisioned with limited roles rather than generic accounts with widely known passwords. The processes for accessing test data should mirror the processes for accessing the live data on which the test data is based.

For more information, see Data Masking Best Practices, an Oracle White Paper on Oracle Technology Network at http://www.oracle.com/technetwork.

For information on column masking and using Oracle Virtual Private Database to control data access, see the Oracle Database Security Guide.

For information on settings and deployment options to protect sensitive data, see the Oracle Fusion Applications Security Hardening Guide.

Masking Formats

Masking formats rely on a PL/SQL function or table of values to pick masked values.

The maximum length of the random string format used to mask data is 4000 characters. For performance reasons, set these strings only as large as necessary to preserve uniqueness on a unique column. For a non-unique column, set the random string smaller.

Random string and number formats are not available in compound masking.

Most masking formats mask the same values in a table consistently. Applying format shuffling on distinct data such as marital status changes the distribution of values (number of records with each value).

Oracle Fusion Applications uses Oracle Data Masking to mask values in a single column consistently across all masking formats rather than mask for generalization to prevent inference-based attacks.

When the group column is specified with a group number the columns from the same table with the same group number are masked consistently.

Oracle Data Masking supports compound masking or tuple masking of a group of columns with the following formats and no conditions.

- Shuffle
- User Defined Function
- Table Column and Substitute formats.

Glossary

abstract role

A description of a person's function in the enterprise that is unrelated to the person's job (position), such as employee, contingent worker, or line manager. A type of enterprise role.

access control

A rule that identifies an entity, an action, and a resource to specify if an action is allowed.

accounting flexfield

The chart of accounts that determines the structure, such as the number and order of individual segments, as well as the corresponding values per segment.

action

The kind of access named in a security policy, such as view or edit.

application identity

Predefined application level user with elevated privileges. An application identity authorizes jobs and transactions for which other users are not authorized, such as a payroll run authorized to access a taxpayer ID while the user who initiated the job is not authorized to access such personally identifiable information.

application role

A role specific to applications and stored in the policy store.

BPEL

Business Process Execution Language; a standard language for defining how to send XML messages to remote services, manipulate XML data structures, receive XML messages asynchronously from remote services, manage events and exceptions, define parallel sequences of execution, and undo parts of processes when exceptions occur.

business object

A resource in an enterprise database, such as an invoice or purchase order.

business unit

A unit of an enterprise that performs one or many business functions that can be rolled up in a management hierarchy.

condition

An XML filter or SQL predicate WHERE clause in a data security policy that specifies what portions of a database resource are secured.

data dimension

A stripe of data accessed by a data role, such as the data controlled by a business unit.

data instance set

The set of human capital management (HCM) data, such as one or more persons, organizations, or payrolls, identified by an HCM security profile.

data role

A role for a defined set of data describing the job a user does within that defined set of data. A data role inherits job or abstract roles and grants entitlement to access data within a specific dimension of data based on data security policies. A type of enterprise role.

data role template

A template used to generate data roles by specifying which base roles to combine with which dimension values for a set of data security policies.

data security

The control of access to data. Data security controls what action a user can taken against which data.

data security policy

A grant of entitlement to a role on an object or attribute group for a given condition.

database resource

An applications data object at the instance, instance set, or global level, which is secured by data security policies.

duty role

A group of function and data privileges representing one duty of a job. Duty roles are specific to applications, stored in the policy store, and shared within an Oracle Fusion Applications instance.

enterprise

An organization with one or more legal entities under common control.

enterprise role

Abstract, job, and data roles are shared across the enterprise. An enterprise role is an LDAP group. An enterprise role is propagated and synchronized across Oracle Fusion Middleware, where it is considered to be an external role or role not specifically defined within applications.

entitlement

Grants of access to functions and data. Oracle Fusion Middleware term for privilege.

flexfield

Grouping of extensible data fields called segments, where each segment is an attribute added to an entity for capturing additional information.

flexfield segment

An extensible data field that represents an attribute on an entity and captures a single atomic value corresponding to a predefined, single extension column in the Oracle Fusion Applications database. A segment appears globally or based on a context of other captured information.

function security

The control of access to a page or a specific widget or functionality within a page. Function security controls what a user can do.

HCM data role

A job role, such as benefits administrator, associated with specified instances of Oracle Fusion Human Capital Management (HCM) data, such as one or more positions or all persons in a department.

HTTP

Acronym for Hypertext Transfer Protocol. A request and response standard typical of client-server computing. In HTTP, web browsers or spiders act as clients, while an application running on the computer hosting the web site acts as a server. The client, which submits HTTP requests, is also referred to as the user agent. The responding server, which stores or creates resources such as HTML files and images, may be called the origin server. In between the user agent and origin server may be several intermediaries, such as proxies, gateways, and tunnels.

identity

A person representing a worker, supplier, or customer.

Java EE

An abbreviation for Java Platform, Enterprise Edition. A programming platform used as the standard for developing multi-tier Java enterprise applications.

job role

A role for a specific job consisting of duties, such as an accounts payable manager or application implementation consultant. A type of enterprise role.

offering

A comprehensive grouping of business functions, such as Sales or Product Management, that is delivered as a unit to support one or more business processes.

personally identifiable information

Any piece of information that can potentially be used to uniquely identify, contact, or locate a single person. Within the context of an enterprise, some PII data can be considered public, such as a person's name and work phone number, while other PII data is confidential, such as national identifier or passport number.

PL/SQL

Abbreviation for procedural structured queried language.

privilege

A grant or entitlement of access to functions and data. A privilege is a single, real world action on a single business object.

role

Controls access to application functions and data.

role hierarchy

Structure of roles to reflect an organization's lines of authority and responsibility. In a role hierarchy, a parent role inherits all the entitlement of one or more child roles.

role mapping

A relationship between one or more job roles, abstract roles, and data roles and one or more conditions. Depending on role-mapping options, the role can be provisioned to or by users with at least one assignment that matches the conditions in the role mapping.

role provisioning

The automatic or manual allocation of an abstract role, a job role, or a data role to a user.

security profile

A set of criteria that identifies one or more human capital management (HCM) objects of a single type for the purposes of securing access to those objects. Security profiles can be defined for persons, organizations, positions, countries, LDGs, document types, payrolls, payroll flows, and workforce business processes.

security reference implementation

Predefined function and data security in Oracle Fusion Applications, including role based access control, and policies that protect functions, data, and segregation of duties. The reference implementation supports identity management, access provisioning, and security enforcement across the tools, data transformations, access methods, and the information life cycle of an enterprise.

segregation of duties

An internal control to prevent a single individual from performing two or more phases of a business transaction or operation that could result in fraud.

SQL predicate

A type of condition using SQL to constrain the data secured by a data security policy.

supplier administrator

An internal job role responsible for maintaining supplier profile data and provisioning supplier contact user accounts.

trading partner

An external party, such as a supplier, in the Oracle B2B application for which electronic documents are sent or from which documents are received. A trading partner in Oracle B2B corresponds to a supplier site.

transaction

A logical unit of work such as a promotion or an assignment change. A transaction may consist of several components, such as changes to salary, locations, and grade, but all the components are handled as a unit to be either approved or rejected.

URL

Abbreviation for uniform resource locator.

XML filter

A type of condition using XML to constrain the data secured by a data security policy.