Oracle Fusion Applications
Understanding Security

Release 8

April 2014
## Contents

### 1 Security Infrastructure

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Components: How They Fit Together</td>
<td>1-1</td>
</tr>
<tr>
<td>Access Components: Explained</td>
<td>1-6</td>
</tr>
<tr>
<td>Security Principles: How They Are Applied</td>
<td>1-7</td>
</tr>
<tr>
<td>Security Processes: How They Are Applied</td>
<td>1-10</td>
</tr>
<tr>
<td>Security Standards: How They Are Applied</td>
<td>1-14</td>
</tr>
<tr>
<td>Security Products: How They Are Applied</td>
<td>1-15</td>
</tr>
<tr>
<td>Secured Oracle Fusion Applications Deployments: Points To Consider</td>
<td>1-18</td>
</tr>
</tbody>
</table>

### 2 Role-Based Access Control

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role-Based Access Control: Explained</td>
<td>2-1</td>
</tr>
<tr>
<td>Role Types: How They Fit Together</td>
<td>2-5</td>
</tr>
<tr>
<td>FAQs for Role Based Access Control</td>
<td>2-7</td>
</tr>
</tbody>
</table>

### 3 Function Security

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function Security: Explained</td>
<td>3-1</td>
</tr>
<tr>
<td>Securing Functions: Points to Consider</td>
<td>3-1</td>
</tr>
</tbody>
</table>

### 4 Data Security

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security: Explained</td>
<td>4-1</td>
</tr>
<tr>
<td>Database Resources and Data Security Policies: How They Work Together</td>
<td>4-4</td>
</tr>
<tr>
<td>Securing Data Access: Points to Consider</td>
<td>4-6</td>
</tr>
<tr>
<td>Data Role Templates: Explained</td>
<td>4-7</td>
</tr>
</tbody>
</table>

### 5 Privacy

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy: Explained</td>
<td>5-1</td>
</tr>
<tr>
<td>Personally Identifiable Information: How It Is Processed</td>
<td>5-7</td>
</tr>
<tr>
<td>Privacy Safeguards: Points To Consider</td>
<td>5-11</td>
</tr>
<tr>
<td>Privacy Breach Prevention and Recovery: Points To Consider</td>
<td>5-13</td>
</tr>
<tr>
<td>FAQs for Privacy</td>
<td>5-14</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforcement Across Tools, Technologies, Data Transformations, and Access Methods: Explained</td>
<td>6-1</td>
</tr>
</tbody>
</table>
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.

Note

If you don’t see any help icons on your page, then click the Show Help icon button in the global area. However, not all pages have help icons.

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. To access the guides, go to any page in Oracle Fusion Applications Help and select Documentation Library from the Navigator menu.

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.

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

For other guides, 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.

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 Send Feedback to Oracle from the Settings and Actions menu in Oracle Fusion Applications Help.
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.

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

**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.

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.

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

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

## 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.

**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 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.
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.

<table>
<thead>
<tr>
<th>Application Identity Code</th>
<th>Application Identity Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>FUSION_APPS_ATK_UMS_APPID</td>
<td>Application Toolkit User Messaging Service Application Identity</td>
</tr>
<tr>
<td>FUSION_APPS_AMX_APPID</td>
<td>Approval Management Service Application Identity</td>
</tr>
<tr>
<td>FUSION_APPS_APM_RGX_APPID</td>
<td>Data Role Template Application Identity</td>
</tr>
<tr>
<td>FUSION_APPS_ECSF_SES_ADMIN_APPID</td>
<td>Oracle Fusion Search Administrator Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_OBIA_BIEE_APPID</td>
<td>Business Intelligence Applications Extract Transform and Load Application Identity</td>
</tr>
<tr>
<td>FUSION_APPS_OIM_SPML_APPID</td>
<td>Oracle Identity Manager Application Identity</td>
</tr>
<tr>
<td>FUSION_APPS_SEARCH_APPID</td>
<td>Oracle Fusion Search Application Identity</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_ADF_APPID</td>
<td>Applications Development Framework Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_ADF_BI_APPID</td>
<td>Applications Development Framework Business Intelligence Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_ADF_SOAP_APPID</td>
<td>Applications Development Framework SOAP Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_DIAGNOSTICS_APPID</td>
<td>Applications Diagnostic Framework Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_ECSF_SEARCH_APPID</td>
<td>Enterprise Search and Crawl Framework Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_EM_APPID</td>
<td>Oracle Enterprise Manager Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_ESD_APPID</td>
<td>Email Sending Daemon Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_ESS_APPID</td>
<td>Enterprise Scheduler Job Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_ESS_REPORT_APPID</td>
<td>Enterprise Scheduler Reporting Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_ODI_ESS_APPID</td>
<td>Oracle Data Integrator Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_ODI_SUPERVISOR_APPID</td>
<td>Oracle Data Integrator Supervisor Application Identity (CRM)</td>
</tr>
<tr>
<td>Application Identity Code</td>
<td>Application Identity Name</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_SELFSERVICE_ADF_APPID</td>
<td>Applications Development Framework Self Service Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_SES_CRAWL_APPID</td>
<td>Oracle Fusion Search Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_CRM_SOA_APPID</td>
<td>Web Services Application Identity (CRM)</td>
</tr>
<tr>
<td>FUSION_APPS_FIN_ADF_APPID</td>
<td>Applications Development Framework Application Identity (Financials)</td>
</tr>
<tr>
<td>FUSION_APPS_FIN_EMPNATID_APPID</td>
<td>Employee National Identifiers Application Identity</td>
</tr>
<tr>
<td>FUSION_APPS_FIN_ESS_EMPMTCH_APPID</td>
<td>Employee Matching Application Identity (Financials)</td>
</tr>
<tr>
<td>FUSION_APPS_FIN_IPM_APPID</td>
<td>Document Management Integration Application Identity (Financials)</td>
</tr>
<tr>
<td>FUSION_APPS_FIN_SOA_APPID</td>
<td>Web Services Application Identity (Financials)</td>
</tr>
<tr>
<td>FUSION_APPS_FSCM_DIAGNOSTICS_APPID</td>
<td>Applications Diagnostic Framework Application Identity (FSCM)</td>
</tr>
<tr>
<td>FUSION_APPS_FSCM_ECSF_SEARCH_APPID</td>
<td>Enterprise Search and Crawl Framework Application Identity (FSCM)</td>
</tr>
<tr>
<td>FUSION_APPS_FSCM_EM_APPID</td>
<td>Oracle Enterprise Manager Application Identity (FSCM)</td>
</tr>
<tr>
<td>FUSION_APPS_FSCM_SES_CRAWL_APPID</td>
<td>Oracle Fusion Search Application Identity (FSCM)</td>
</tr>
<tr>
<td>FUSION_APPS_HCM_DIAGNOSTICS_APPID</td>
<td>Applications Diagnostic Framework Application Identity (HCM)</td>
</tr>
<tr>
<td>FUSION_APPS_HCM_ECSF_SEARCH_APPID</td>
<td>Enterprise Search and Crawl Framework Application Identity (HCM)</td>
</tr>
<tr>
<td>FUSION_APPS_HCM_EM_APPID</td>
<td>Oracle Enterprise Manager Application Identity (HCM)</td>
</tr>
<tr>
<td>FUSION_APPS_HCM_ESS_APPID</td>
<td>Enterprise Scheduler Job Application Identity (HCM)</td>
</tr>
<tr>
<td>FUSION_APPS_HCM_ESS_LOADER_APPID</td>
<td>Batch Loader Enterprise Scheduler Job Application Identity (HCM)</td>
</tr>
<tr>
<td>FUSION_APPS_HCM_ODI_ESS_APPID</td>
<td>Oracle Data Integrator Application Identity (HCM)</td>
</tr>
<tr>
<td>Application Identity Code</td>
<td>Application Identity Name</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-------------------------------------------------------------------</td>
</tr>
<tr>
<td>FUSION_APPS_HCM_ODI_SUPERVISOR_APPID</td>
<td>Oracle Data Integrator Supervisor Application Identity (HCM)</td>
</tr>
<tr>
<td>FUSION_APPS_HCM_SES_CRAWL_APPID</td>
<td>Oracle Fusion Search Application Identity (HCM)</td>
</tr>
<tr>
<td>FUSION_APPS_HCM_SOA_APPID</td>
<td>Web Services Application Identity (HCM)</td>
</tr>
<tr>
<td>FUSION_APPS_HCM_SOA_SPML_APPID</td>
<td>Service Provisioning Markup Language Interface Application Identity (HCM)</td>
</tr>
<tr>
<td>FUSION_APPS_WCFORUM_ADMIN_APPID</td>
<td>Web Center Forum Application Identity</td>
</tr>
<tr>
<td>FUSION_APPS_WEBCENTER_CRAWL_APPID</td>
<td>Oracle WebCenter Crawl Application Identity</td>
</tr>
<tr>
<td>FUSION_APPS_WSM_APPID</td>
<td>Web Services Manager Application Identity</td>
</tr>
<tr>
<td>FUSION_APPS_PRC_ADF_APPID</td>
<td>Applications Development Framework Application Identity (Procurement)</td>
</tr>
<tr>
<td>FUSION_APPS_PRC_ESS_APPID</td>
<td>Enterprise Scheduler Job Application Identity (Procurement)</td>
</tr>
<tr>
<td>FUSION_APPS_PRC_SOA_APPID</td>
<td>Web Services Application Identity (Procurement)</td>
</tr>
<tr>
<td>FUSION_APPS_PRJ_ADF_APPID</td>
<td>Applications Development Framework Application Identity (Projects)</td>
</tr>
<tr>
<td>FUSION_APPS_PRJ_ESS_APPID</td>
<td>Enterprise Scheduler Job Application Identity (Projects)</td>
</tr>
<tr>
<td>FUSION_APPS_PRJ_SOA_APPID</td>
<td>Web Services Application Identity (Projects)</td>
</tr>
<tr>
<td>FUSION_APPS_SCM_ADF_APPID</td>
<td>Applications Development Framework Application Identity (SCM)</td>
</tr>
<tr>
<td>FUSION_APPS_SCM_ESS_APPID</td>
<td>Enterprise Scheduler Job Application Identity (SCM)</td>
</tr>
<tr>
<td>FUSION_APPS_SCM_SOA_APPID</td>
<td>Web Services Application Identity (SCM)</td>
</tr>
<tr>
<td>FUSION_APPS_SETUP_ESS_APPID</td>
<td>Enterprise Scheduler Job Application Identity (Setup)</td>
</tr>
</tbody>
</table>

**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:

```bash
Ldapsearch -h ldapHost -p ldapPort -D binddn -w password -b 'cn=appidusers,cn=users,namingcontext' -s sub 'objectclass=orclAppiduser' cn >& reset.txt
ORACLE_HOME/idmtools/bin/appidtool.sh pwdreset -ldapHost tuvwx0123.us.example.com -ldapPort 3060 -ldapUser cn=orcladmin -wlsHost tuvwx0123.us.example.com -wlsPort 7001 -wlsUser weblogic -file reset.txt -userBase cn=users,namingcontext
```

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

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.
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.

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.
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.
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.

<table>
<thead>
<tr>
<th>Data security feature</th>
<th>Does what?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data security policy</td>
<td>Grants access to roles by means of entitlement</td>
</tr>
</tbody>
</table>
Data security feature | Does what?
---|---
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.

<table>
<thead>
<tr>
<th>Who</th>
<th>can do</th>
<th>what</th>
<th>on which set of data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts payable managers</td>
<td>view</td>
<td>AP disbursements</td>
<td>for their business unit</td>
</tr>
</tbody>
</table>

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.
Data Security 4-3

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.

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.

<table>
<thead>
<tr>
<th>Method of securing data</th>
<th>Reason</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data roles apply explicit data security policies on job and abstract roles</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Data security policies</td>
<td>Define data access for application roles and provide inheriting job and abstract roles with implicit data security</td>
<td>Projects</td>
</tr>
</tbody>
</table>

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).
Oracle Fusion Applications Understanding Security

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.
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.

<table>
<thead>
<tr>
<th>PII Classification</th>
<th>Protected in Oracle Fusion Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>No</td>
</tr>
<tr>
<td>Public within the enterprise</td>
<td>User interface</td>
</tr>
</tbody>
</table>
Table 5-2: Oracle Fusion Applications Understanding Security

<table>
<thead>
<tr>
<th>PII Classification</th>
<th>Protected in Oracle Fusion Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential</td>
<td>User interface and database</td>
</tr>
</tbody>
</table>

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 example, 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 PII 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.

<table>
<thead>
<tr>
<th>PII Attribute</th>
<th>Public no additional security</th>
<th>Public within the enterprise: secure in the user interface</th>
<th>Confidential: secure in the user interface and database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Article Number</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank Account Number</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometrics Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Email Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Telephone Number</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card Number: Credit or Debit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PII Attribute</td>
<td>Public: no additional security</td>
<td>Public within the enterprise: secure in the user interface</td>
<td>Confidential: secure in the user interface and database</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Citizenship Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Civil Identifier Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Club Membership ID</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Custom Name</td>
<td>Yes (Recruiter in HCM Recruiting System)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Digital ID</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Drivers License Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Electronic Taxpayer ID</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Employee Number</td>
<td>Yes (Recruiter in HCM Recruiting System)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Government Affiliation ID</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>GPS Location</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Hafiza Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Health Insurance Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Identity Card Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Instant Messaging Address</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Library Card Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Maiden Name</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Mail Stop</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Medical Information</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Military Service ID</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>National Identifier</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>PII Attribute</td>
<td>Public: no additional security</td>
<td>Public within the enterprise: secure in the user interface</td>
<td>Confidential: secure in the user interface and database</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Party Number or Customer Number</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Passport Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Pension ID Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Pension Registration Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Person Identification Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Person Name</td>
<td>Yes (Name of recruiter in HCM Recruiting System)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Personal Address</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Personal Email Address</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Personal Public Service Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Residency Number (Green Card)</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Social Insurance Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Social Security Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Student Examination Hall Ticket Number</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Tax Registration Number or National Taxpayer Identifier</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Trade Union Membership Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Unemployment Insurance Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>User Global Identifier</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Visa Number or Work Permit</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>PII Attribute</td>
<td>Public: no additional security</td>
<td>Public within the enterprise: secure in the user interface</td>
<td>Confidential: secure in the user interface and database</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Voter Identification Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Web Site</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Welfare Pension Insurance Number</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Sensitive Attribute Category</th>
<th>Public</th>
<th>Internal Public</th>
<th>Confidential Restricted</th>
<th>Confidential Highly Restricted</th>
<th>Type</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unannounced Financial Results</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>Commercial</td>
<td></td>
</tr>
<tr>
<td>Financial Forecasts</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>Commercial</td>
<td></td>
</tr>
<tr>
<td>Competitive Analysis</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>Commercial</td>
<td></td>
</tr>
<tr>
<td>Strategic Business Plans</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>Commercial</td>
<td></td>
</tr>
<tr>
<td>Product design specifications</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>Commercial</td>
<td></td>
</tr>
<tr>
<td>Compensation</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>Personal</td>
<td>Salary, bonus, stock, bank and account information, retirement accounts</td>
</tr>
<tr>
<td>Sensitive Attribute Category</td>
<td>Public</td>
<td>Internal Public</td>
<td>Confidential Restricted</td>
<td>Confidential Highly Restricted</td>
<td>Type</td>
<td>Use</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------</td>
<td>-----------------</td>
<td>------------------------</td>
<td>-------------------------------</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>Employment details</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td>Personal</td>
<td>Performance evaluation, grade, ranking, hire date, background checks and security clearances</td>
</tr>
<tr>
<td>Nationality and Citizenship</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td>Personal</td>
<td>Including work permit information</td>
</tr>
<tr>
<td>Health Information</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td>Personal</td>
<td>Disability leave, health care providers and plans, medical information</td>
</tr>
<tr>
<td>Personal information</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td>Personal</td>
<td>Birth date, place of birth, race and ethnicity, medical information, religion, politics, sexual orientation, union membership, offenses, race and ethnicity</td>
</tr>
<tr>
<td>Mother’s maiden name</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td>Personal</td>
<td></td>
</tr>
<tr>
<td>Passwords</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td>Security</td>
<td>Including access code or PIN</td>
</tr>
<tr>
<td>Encryption keys</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Customer configuration</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td>Security</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>PII</th>
<th>Confidential PII</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Private Address Details</td>
</tr>
<tr>
<td>Drivers License Number</td>
<td>Drivers License Number</td>
</tr>
<tr>
<td>Article Number</td>
<td>Private Email Details</td>
</tr>
<tr>
<td>Civil Identifier Number</td>
<td>Civil Identifier Number</td>
</tr>
<tr>
<td>Civil Registration Number</td>
<td>Civil Registration Number</td>
</tr>
<tr>
<td>GOSI Number</td>
<td>GOSI Number</td>
</tr>
<tr>
<td>Government Affiliation ID</td>
<td>Government Affiliation ID</td>
</tr>
<tr>
<td>Hafiza Number</td>
<td>Hafiza Number</td>
</tr>
<tr>
<td>Military Service ID</td>
<td>Military Service ID</td>
</tr>
<tr>
<td>National Identifier</td>
<td>National Identifier</td>
</tr>
<tr>
<td>National Taxpayer Identifier (NIP)</td>
<td>National Taxpayer Identifier (NIP)</td>
</tr>
<tr>
<td>Nationality Number</td>
<td>Nationality Number</td>
</tr>
<tr>
<td>Pension ID Number</td>
<td>Pension ID Number</td>
</tr>
<tr>
<td>Social Insurance Number</td>
<td>Social Insurance Number</td>
</tr>
<tr>
<td>PII</td>
<td>Confidential PII</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>Social Security Number</td>
</tr>
<tr>
<td>Personal Public Service Number</td>
<td></td>
</tr>
<tr>
<td>RFC ID</td>
<td></td>
</tr>
<tr>
<td>Tax Registration Number or National Taxpayer Identifier</td>
<td>Tax Registration Number</td>
</tr>
<tr>
<td>Unemployment Insurance Number</td>
<td>Unemployment Insurance Number</td>
</tr>
<tr>
<td>Passport Number</td>
<td>Passport Number</td>
</tr>
<tr>
<td>Person Name</td>
<td></td>
</tr>
<tr>
<td>Maiden Name</td>
<td></td>
</tr>
<tr>
<td>Telephone Number</td>
<td>Private Phone Details</td>
</tr>
<tr>
<td>Iqama Number</td>
<td>Iqama Number</td>
</tr>
<tr>
<td>Visa Number</td>
<td>Visa Number</td>
</tr>
<tr>
<td>Visa Number or Work Permit</td>
<td>Visa Number or Work Permit</td>
</tr>
</tbody>
</table>

**How PII is Processed**

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

<table>
<thead>
<tr>
<th>Data Attribute</th>
<th>Business Object</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Identifier Oracle Fusion Expenses</td>
<td>Corporate Card</td>
<td>Used to match new card not previously matched to employee</td>
</tr>
<tr>
<td>Bank Account Number in Oracle Fusion Payments</td>
<td>External Bank Account (LE)</td>
<td>Column subject to PCI/PABP in addition to PII security</td>
</tr>
<tr>
<td></td>
<td>Disbursement (LE)</td>
<td>Masked payee bank account number, denormalized from IBY_EXT_BANK_ACCOUNTS_ALL; column subject to PCI/PABP in addition to PII security</td>
</tr>
<tr>
<td></td>
<td>Disbursement (LE)</td>
<td>Masked payee bank account number, denormalized from IBY_EXT_BANK_ACCOUNTS_ALL; column subject to PCI/PABP in addition to PII security</td>
</tr>
<tr>
<td>Data Attribute</td>
<td>Business Object</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>----------</td>
</tr>
<tr>
<td>Card Number in Oracle Fusion Payments</td>
<td>Payment Card (LE)</td>
<td>Column subject to PCI/PABP in addition to PII security</td>
</tr>
<tr>
<td>Tax Registration Number in Oracle Fusion Tax</td>
<td>Detail Tax Line (LE)</td>
<td>Tax Registration Number for external parties; may contain personal TRN</td>
</tr>
<tr>
<td>Tax Registration (LE)</td>
<td>Tax Registration Number for external parties; may contain personal TRN. This attribute is indexed and search identifies non-equality.</td>
<td></td>
</tr>
<tr>
<td>Party Tax Profile (LE)</td>
<td>Tax Registration Number for external parties; may contain personal TRN</td>
<td></td>
</tr>
<tr>
<td>Tax Registration Number in Oracle Fusion Expenses</td>
<td>Expense</td>
<td>Taxpayer Identifier of the merchant with which employee conducted the transaction</td>
</tr>
<tr>
<td>Corporate Card Transaction</td>
<td>Taxpayer Identifier of the merchant with which employee conducted the transaction</td>
<td></td>
</tr>
<tr>
<td>National Taxpayer Identifier in Oracle Fusion Financials for EMEA</td>
<td>Spanish Withholding Interface (LE)</td>
<td>Supplier Taxpayer Identifier, used for Spanish Withholding Tax functionality</td>
</tr>
<tr>
<td>National Taxpayer Identifier in Oracle Fusion Expenses</td>
<td>Expense</td>
<td>Taxpayer Identifier of the merchant with which employee conducted the transaction</td>
</tr>
<tr>
<td>Corporate Card Transaction</td>
<td>Taxpayer Identifier of the merchant with which employee conducted the transaction (column name may be sync up with previous entry)</td>
<td></td>
</tr>
</tbody>
</table>

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 that 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.
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.

<table>
<thead>
<tr>
<th>Change</th>
<th>Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Application Development Framework (ADF)</td>
</tr>
<tr>
<td></td>
<td>Enterprise Scheduling Systems</td>
</tr>
<tr>
<td></td>
<td>Hyperion SmartView</td>
</tr>
<tr>
<td></td>
<td>Oracle Business Intelligence</td>
</tr>
<tr>
<td></td>
<td>Universal Content Management</td>
</tr>
<tr>
<td></td>
<td>Web Center</td>
</tr>
<tr>
<td>New Job With Existing Duties</td>
<td>1 1 1 1 1 1 1 1 1 1</td>
</tr>
<tr>
<td>New Job With New Duties</td>
<td>2 2 2 4 1 4 1 4</td>
</tr>
<tr>
<td>Existing Duty Change to Existing Entitlement</td>
<td>3 3 3 3 1 3</td>
</tr>
<tr>
<td>New Duty With Existing Entitlement</td>
<td>3 3 4 4 1 4</td>
</tr>
<tr>
<td>Existing Duty With New Entitlement</td>
<td>4 4 4 4 1 4</td>
</tr>
<tr>
<td>New Duty With New Entitlements</td>
<td>4 4 4 4 1 4 1 4</td>
</tr>
<tr>
<td>Existing Entitlement With Existing Permissions</td>
<td>5 5 5 5 1 5</td>
</tr>
<tr>
<td>New Entitlement With Existing Permissions</td>
<td>6 6 6 6 1 6</td>
</tr>
<tr>
<td>New Entitlement With New Permissions</td>
<td>7 7 7 7 1 7</td>
</tr>
</tbody>
</table>

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 policies 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 a 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 give 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.

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.

<table>
<thead>
<tr>
<th>User Type</th>
<th>Job Role</th>
<th>Navigation to Work Area (Path)</th>
<th>BPM Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Producer</td>
<td>Product Manager</td>
<td>Product Management &gt; Items</td>
<td>Create Item</td>
</tr>
<tr>
<td>Consumer</td>
<td>Warehouse Manager</td>
<td>Warehouse Operations &gt; Inventory</td>
<td>Create Item</td>
</tr>
<tr>
<td>Consumer</td>
<td>Cost Accountant</td>
<td>Costing &gt; Cost Accounting</td>
<td>Create Item</td>
</tr>
</tbody>
</table>

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.
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 provisioning 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.
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.


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)
Oracle Fusion Applications Understanding Security 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.

**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.

<table>
<thead>
<tr>
<th>Common Extension</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>New job with existing duties</td>
<td>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.</td>
</tr>
<tr>
<td>Existing duty with different existing entitlement</td>
<td>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.</td>
</tr>
<tr>
<td>New duty with existing entitlement</td>
<td>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.</td>
</tr>
<tr>
<td>New hierarchy with existing duties</td>
<td>Create new hierarchies of existing duties to reflect the access required by the job roles in your enterprise.</td>
</tr>
<tr>
<td>New job with new duties</td>
<td>Create new job roles and new duty roles for providing access to custom applications.</td>
</tr>
</tbody>
</table>

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 Application Composer and securing new business objects in an extended application, see the Oracle Fusion Applications Extensibility Guide for Developers.

**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.
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.
Secure 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.

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Life Cycle Phase</th>
<th>Protection provided by:</th>
<th>Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Fusion</td>
<td>All</td>
<td>Access restrictions and</td>
<td>Oracle Database Vault, single realm</td>
</tr>
<tr>
<td>Application data</td>
<td></td>
<td>segregation of duties</td>
<td></td>
</tr>
<tr>
<td>Sensitive</td>
<td>Installation</td>
<td>Transparent data encryption</td>
<td>Oracle Advanced Security (OAS) and TDE</td>
</tr>
<tr>
<td></td>
<td>Implementation</td>
<td>Transparent data encryption</td>
<td>OAS and TDE</td>
</tr>
<tr>
<td></td>
<td>Test</td>
<td>Data Masking</td>
<td>Oracle Data Masking</td>
</tr>
<tr>
<td></td>
<td>Production and change</td>
<td>Transparent data encryption</td>
<td>OAS and TDE</td>
</tr>
<tr>
<td></td>
<td>control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Archive and purge</td>
<td>Transparent data encryption</td>
<td>OAS and TDE</td>
</tr>
<tr>
<td></td>
<td>Data at rest</td>
<td>Transparent data encryption</td>
<td>OAS and TDE</td>
</tr>
<tr>
<td></td>
<td>Data in transit</td>
<td>Network encryption</td>
<td>Network Data Encryption and Data Integrity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>features of Oracle Advanced Security</td>
</tr>
</tbody>
</table>

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.

Locking Down Web Services: Points to Consider

Oracle Fusion Web Services are set up with internal and external policies.

All internal-facing Web services are protected by Authentication Only policies.

<table>
<thead>
<tr>
<th>Service or Client Side</th>
<th>Internal Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Side</td>
<td>oracle/wss_saml_or_username_token_service_policy</td>
<td>The service accepts an unencrypted username and password token, or an unsigned Security Assertions Markup Language (SAML) token.</td>
</tr>
<tr>
<td>Client Side</td>
<td>oracle/wss_username_token_client_policy</td>
<td>The client sends an unencrypted username and password.</td>
</tr>
<tr>
<td>Client Side</td>
<td>oracle/wss10_saml_token_client_policy</td>
<td>The client sends unsigned SAML token.</td>
</tr>
</tbody>
</table>
These policies send and accept passwords in clear text, meaning unencrypted. They do not perform any encryption or signing, and they do not have high security. However, they are high performance because they don’t do any expensive cryptography operations. They should be used only for backend Web services in small internal private networks that are completely blocked off from the internet and also blocked off from the enterprise intranet.

External-facing web services are protected by WS11 Message protection policies.

<table>
<thead>
<tr>
<th>Service or Client Side</th>
<th>External Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Side</td>
<td>oracle/wss11_saml_or_username_token_with_message_protection_service_policy</td>
<td>The service accepts encrypted username and password token, or a signed SAML token, plus the entire message body must be signed and encrypted.</td>
</tr>
<tr>
<td>Client Side</td>
<td>oracle/wss11_username_token_with_message_protection_client_policy</td>
<td>The client sends an encrypted username and password.</td>
</tr>
<tr>
<td>Client Side</td>
<td>oracle/wss11_saml_token_with_message_protection_client_policy</td>
<td>The client sends signed SAML token.</td>
</tr>
</tbody>
</table>

These policies are very secure, however they are not high performance because they do expensive cryptographic operations.

Oracle Fusion Applications provisioning also sets the following policies globally at the domain level.

<table>
<thead>
<tr>
<th>Service or Client Side</th>
<th>Global Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Side</td>
<td>oracle/wss_saml_or_username_token_service_policy</td>
<td>The authentication only policy.</td>
</tr>
<tr>
<td>Client Side</td>
<td>oracle/wss10_saml_token_client_policy</td>
<td>The authentication only policy for SAML token.</td>
</tr>
</tbody>
</table>

Since these are set globally on the domain level, all Web services and Web service clients automatically get these policies unless they attach a different policy locally. Since the global policy attachment (GPA) policy is set to Authentication only, all internal-facing services use this GPA policy, whereas all the external-facing services attach their message protection policy locally.

The message protection policies also need a keystore. The Oracle Fusion Applications provisioning script sets up an initial keystore with the name default-keystore.jks that contains a single private key and a self-signed certificate with alias orakey. All but the Oracle Identity Management (OIM) domain are set up with this same keystore, which means that all the Oracle Fusion Applications domains, except OIM, share this same key.

The following figure shows that each domain of a deployment provides access to identity management using the default Java keystore (JKS) default_keystore.jks. Each default keystore file contains an identical, single key called orakey. The credentials store based on a Lightweight Directory Access Protocol (LDAP) such
as Oracle Internet Directory (OID) in the Oracle Identity Management domain stores the keystore and key passwords and is shared across all domains.

Configuring External Clients to Communicate with Externally Facing Web Services

Since external Web services are protected by the external service oracle/wssl_saml_or_username_token_with_message_protection_service_policy, external clients need to either provide username and password or a SAML assertion.

External clients must complete the following steps.

- Get the certificate of the service.
  
  The certificate is advertised in the Web Services Description Language (WSDL). To extract the certificate from the WSDL, perform the following steps.
  
  a. Save the WSDL to a local file.
  
  b. Search for the string <X509Certificate> inside the local file to locate the certificate.

  For example,

  <dsig:X509Certificate> MIICHTCCAYagAwIBAgIETBwVYjA ... </dsig:X509Certificate>
c. Copy this long string framed by the `<dsig:X509Certificate>` tags into a text file.

d. Rename the file.
   1. If you are using this certificate in a Microsoft client, you can rename this file with .cer file extension and use it as a certificate file.
   2. If you are using this certificate in a Java client, change the text file so that the certificate is framed by `BEGIN` and `END`. For example,

```
-----BEGIN MIICHTCCAYagAwIBAgIETBwVYjA ...
-----END
```

- Import the certificate of the service into your client’s trust store.
   - For Java clients use `keytool -importcert` to import this file from the previous step into your client’s keystore.
- [For SAML only.] Generate a client certificate.
   - If your client expects to perform ID propagation, the client needs to authenticate with SAML certificates. For this the client needs to have a client certificate for use as a SAML signing key.
- [For SAML only.] Import the client certificate into the trust store of the service.
   - Take the certificate in the previous step and import it into the default-keystore.jks file of the service.

**Warning**

A SAML signing key lets the client authenticate as any user, so SAML is recommended for trusted clients that need to propagate user identities. Regular clients should use username and password instead of SAML.

**Hardening Web Services**

For more security you can make the following adjustments.

- Choose a more secure policy for all your internal Web services. You may choose to not distinguish between internal and external, and use the same policy for all Web services.
- Change your keystore to have private keys and certificates. For example if you have an enterprise certificate authority (CA), you can use that to generate your keys, and put the CA certificate in the keystore.

**Caution**

When changing the attachment of the security policies, the client policy

Be aware of the following fundamentals when changing the attachment of the security policies.

- The client and callback policies must be compatible with the service that you are invoking, otherwise the Web service invocation will not work.
• In the case of export setup data, the corresponding Service and Callback policies for all Setup Data services must match the Functional Setup Manager (FSM) Processing Service (MigratorService) and FSM Migrator Callback Service (MigratorCallbackService) policies. These must be the same in all the domains so that FSM export and import are fully functional.

• As a security guideline, use the same GPA policy across all the domains if you change the domain-wide GPA policy.

If you use a secure sockets layer (SSL) policy, verify the following.

• You have set the Oracle HTTP Server (OHS) options to propagate the SSL client certificate and settings to the Weblogic Server (WLS) if your SSL terminates at the OHS.

For more information on setting up your environment for policies, see the Oracle Fusion Middleware Security and Administrator’s Guide for Web Services.

• You have set the SSL variables and client to go to OHS and then load balancer (LBR) if your SSL terminates at the LBR level.

• You have configured the policies for SAML Token (Sender Vouches) Over SSL for two-way SSL. Other authentication tokens such as username token, SAML bearer token, and so on, require only one-way SSL.

For information about securing Web services generally, see the Oracle Fusion Application Administrator’s Guide.

**More Secure Keys and Certificates**

Oracle Fusion Applications provisioning sets up the keystore with self-signed certificates that you can choose to replace your own keys and certificates.

For example, if you have an enterprise CA, you can use that to generate keys and certificates, but you must also do the following.

• Configure your Web services to accept only a configured list of SAML signers by configuring the trusted distinguished names (DN) list for SAML signing certificates in every domain.

The private key that you configure for Oracle Web Services Manager (OWSM) is used for signing SAML Sender Vouches assertion. The certificates that you place in the OWSM keystore are for verifying SAML assertion. If you put your enterprise CA in this OWSM keystore, every certificate issued by your enterprise is acceptable for verifying assertion unless Web services is configured to accept only your list of SAML signers.

For more information about Defining a Trusted Distinguished Names List for SAML Signing Certificates, see the Oracle Fusion Middleware Security and Administrator’s Guide for Web Services.

• Enable hostname verification by setting the value of wsm.ignore.hostname.verification to false.

By default, host name verification is turned off in OWSM.
Hardware Security Modules

Hardware security modules (HSM) protect high-value cryptographic keys on the application server. For example, you can use an HSM together with Oracle Transparent Data Encryption to store the master encryption key.

As a security guideline, secure Web services that are served through HTTPS (SSL/TLS) by using SSL Acceleration HSMs.

Network Security

Network Security: Overview

The enterprise deployment guidelines stipulate a network configuration discipline to ensure security at all needed levels.

The following reasons may prevent you from matching the topology and network arrangements described in the enterprise deployment guidelines.

- You need to leverage an existing network arrangement and do not have the flexibility to make topology changes.
- You have higher levels of risk aversion due to compliance requirements such as for government or defense, or your industry segment requires special regulatory compliance and audit considerations.

For these reasons and given your deployment scenario you may not find it prudent for back-channel communications to occur in the "clear." As an alternative, you can implement SSL-based network encryption.

Note

SSL-based network encryption introduces greater complexity to your enterprise deployment, which affects performance.

Deployment administrators secure back-channel networks by choosing SSL where necessary and also tightening the security policies of their Web services that are independent of SSL.

Network Security in Oracle Fusion Applications Enterprise Deployments: Explained

The objective of network security is to prevent exposure of data transmitted over the network to unauthorized users and also to prevent malicious "person in the middle" attacks.

The following methods are most common in achieving network security.

- Configuring Secure Socket Layer (SSL) on all network connections among servers, as well as between clients and servers.
• Isolating the servers involved within their own isolated networks or protected network zones, which are only accessible by authorized administrators.

For mission critical enterprise applications such as Oracle Fusion Applications, a judicious combination of both of these schemes is considered ideal for ensuring not only security, but also ease of deployment and maintenance. The architectures of the enterprise deployment guidelines rely on this hybrid strategy. You must understand the built-in network security model offered by the enterprise deployment guidelines to understand the scenarios where you could consider additional SSL configurations and other network security measures.

As the guiding network security principle of most deployments, the middleware servers for Oracle Fusion Applications run on an isolated network within the larger corporate network. Accordingly, Enterprise Deployment Architecture (EDA) stipulates network isolation for various functional groups. Each functional group of software components is isolated in its own firewall separated by demilitarized zones (DMZ). All traffic is restricted by protocol and port. SSL is configured to secure all the network segments between Oracle Fusion Application components and enterprise infrastructures outside of the Oracle Fusion Application functional groups.

The network architecture of the enterprise deployment guidelines includes the following.

• The Web servers (Oracle HTTP Server (OHS)), the application servers (WebLogic Server (WLS)), and all other servers for your Oracle Fusion Applications instance run within a single isolated network.

• The Oracle Fusion Applications Database, Oracle Business Intelligence, Oracle WebCenter Content Management, and Oracle Fusion Applications Search services all run in either the same isolated network or each in its own isolated network that can only be reached via the applications private network.

• Centralized services such as Oracle Identity Management (OIM) servers are assumed to operate outside of these isolated networks.

• The connection to the database is assumed to be between two isolated networks.

• There are no connections to external Web services configured by initial provisioning.

Given that this network topology is the target, the enterprise deployment guidelines recommend enabling SSL appropriately for all connections leading into or out of the isolated networks.

The figure shows the connections that are SSL enabled in an Oracle Fusion Applications deployment. The connections among the Oracle WebLogic Servers (WLS) and domains of the Oracle Fusion Applications deployment are not SSL enabled because the enterprise deployment guidelines require and assume that the subnets in the data center where Oracle Fusion Application is deployed are secured by network firewalls preventing direct access of Oracle Fusion Application components by users and applications outside the data center. The connection to the Oracle Fusion Applications database in an adjoining protected zone is also not SSL enabled. But connections to the identity access management components are SSL enabled.
For more information on configuring SSL in the generic case, see the Oracle Fusion Applications Administrator’s Guide.

**Network Security on Oracle Fusion Applications Search: Points to Consider**

Oracle Fusion Applications enforces security in Oracle Fusion Applications Search and the Enterprise Crawl and Applications Search Framework (ECSF).

Oracle Fusion Applications Search can be further hardened by enabling a secure sockets layer (SSL).

**Hardening Oracle Fusion Applications Search**

When enabling SSL in an Oracle Fusion Applications environment, the keystore certificate and the following system properties must be set for the crawler in Oracle Fusion Applications Search.

**Settings for Oracle Fusion Applications Search with SSL Enabled on Windows**

Ensure that the crawler script file `%ORACLE_HOME%\bin\crawlerlauncher.cmd` contains the following line after the set `PATH=` line.
set TRUST_STORE_PATH=%WEBLOGIC_HOME%\server\lib\fusion_trust.jks

Ensure that the following properties are included both in the CRAWLER_EXEC_PARAMS script variable and in the Java command at the end of the script file.

-Dweblogic.security.SSL.trustedCAKeyStore=%TRUST_STORE_PATH%
-Djavax.net.ssl.trustStore=%TRUST_STORE_PATH%

Settings for Oracle Fusion Applications Search with SSL Enabled on Linnux

Ensure that the crawler script file $ORACLE_HOME/bin/crawlerlauncher.sh contains the following line after the LOG_PREFIX= line.

TRUST_STORE_PATH=$WLS_HOME/server/lib/fusion_trust.jks

Ensure that the following properties are included both in the CRAWLER_EXEC_PARAMS script variable and in the Java command at the end of the script file.

-Dweblogic.security.SSL.trustedCAKeyStore=$TRUST_STORE_PATH
-Djavax.net.ssl.trustStore=$TRUST_STORE_PATH

For more information about SSL and HTTPS Support in Oracle Fusion Applications Search, see the Oracle Secure Enterprise Applications Search Administrator’s Guide.

Advanced Security

Advanced Security : Explained

Oracle Database offers advanced security features and guidelines to match higher levels of security requirements for a range of reasons.

Industry segment or organization type of the enterprise may impose regulatory requirements that determine how much risk is tolerable or how much to harden the deployment.

Protecting Sensitive Data

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

The table shows security features used for various requirements and hardening goals.

<table>
<thead>
<tr>
<th>Security Requirement</th>
<th>Hardening target</th>
<th>Hardening Reason</th>
<th>Security Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protecting sensitive data</td>
<td>Data beyond the PII defined by Oracle Fusion Applications</td>
<td>If access is gained to the file system or backups the data cannot be read.</td>
<td>Transparent Data Encryption Protecting sensitive data from DBAs</td>
</tr>
<tr>
<td>Security Requirement</td>
<td>Hardening target</td>
<td>Hardening Reason</td>
<td>Security Feature</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Protecting sensitive data from DBAs</td>
<td>Data beyond the PII defined by Oracle Fusion Applications</td>
<td>DBA access is not be subject to security policies in Oracle Platform Security Services (OPSS) and should therefore be limited or blocked through other means.</td>
<td>Oracle Data Vault and Oracle Audit Vault</td>
</tr>
<tr>
<td>Protecting sensitive data in clones</td>
<td>Data beyond the PII specified by the data masking templates defined in Oracle Enterprise Manager, integrated with Oracle Fusion Applications</td>
<td>Developers need realistic test data to test modifications and configurations. Such test data should be easy to construct, should test the real boundaries of the data, and should not allow developers to access information in the test environment that they would not be authorized to access in a live environment, except where there is a specific business reason for them to do so. Even when the data has been masked, access to it should be rigorously controlled, and all users made aware of their obligations and responsibilities with regard to it.</td>
<td>Oracle Data Masking</td>
</tr>
<tr>
<td>Protecting sensitive data in transit</td>
<td>Data beyond the PII protected by the enterprise deployment guidelines of Oracle Fusion Applications</td>
<td>Network security (instead or in addition to SSL)</td>
<td></td>
</tr>
</tbody>
</table>

**Data Encryption: Points to Consider**

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**

For encryption beyond the Oracle Fusion Applications encryption application programming interfaces (APIs) protections on data such as credit card numbers...
in application user interface fields, Transparent Data Encryption (TDE) is certified but optional with Oracle Fusion Applications.

TDE enables encrypting data independent of managing encryption keys. TDE supports encryption at the tablespace level. Encrypting an entire tablespace automatically encrypts all objects created in that tablespace, including sensitive data. You do not have to analyze and determine the need for encryption on individual table columns.

**Tablespace Level Encryption**

Use TDE at the tablespace level to maintain an optimal balance between performance and security.

TDE encrypts sensitive table data stored in data files at the tablespace level. The following table lists the tablespaces and the types of objects in Oracle Fusion Applications.

<table>
<thead>
<tr>
<th>Logical Tablespace Type</th>
<th>Physical Tablespace</th>
<th>Object Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUMMARY</td>
<td>FUSION_TS_SUMMARY</td>
<td>Materialized Views (MV), MV logs</td>
</tr>
<tr>
<td>TRANSACTION_TABLES</td>
<td>FUSION_TS_TX_DATA</td>
<td>Transactional tables</td>
</tr>
<tr>
<td>TRANSACTION_INDEXES</td>
<td>FUSION_TS_TX_IDX</td>
<td>Indexes on transactional tables</td>
</tr>
<tr>
<td>REFERENCE</td>
<td>FUSION_TS_SEED</td>
<td>Setup and seed tables</td>
</tr>
<tr>
<td>INTERFACE</td>
<td>FUSION_TS_ARCHIVE</td>
<td>Interface tables</td>
</tr>
<tr>
<td>MEDIA</td>
<td>FUSION_TS_MEDIA</td>
<td>Tables with multimedia objects, such as text, video, sound, graphics, and spatial data</td>
</tr>
<tr>
<td>TOOLS</td>
<td>FUSION_TS_TOOLS</td>
<td>Tables that are part of other 3rd party products and tools</td>
</tr>
<tr>
<td>ARCHIVE</td>
<td>FUSION_TS_ARCHIVE</td>
<td>Obsolete tables and objects</td>
</tr>
<tr>
<td>TEMPORARY</td>
<td>TEMP</td>
<td>Global temporary tables</td>
</tr>
<tr>
<td>AQ</td>
<td>FUSION_TS_QUEUES</td>
<td>AQ$ and its related tables (_H, _I, _T, _S, _R)</td>
</tr>
</tbody>
</table>

**Data Masking: Points to Consider**

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.

**Oracle Data Masking**

Oracle Data Masking is available for masking data in non-production instances or clones.

Oracle Fusion Applications Data Masking templates apply masking formats on sensitive data in clones. Change the list of sensitive attributes to be masked by Oracle Data Masking using Oracle Enterprise Manager.

**Masking Definitions**

For masking beyond the encryption application programming interfaces (APIs) protections on data such as credit card numbers in application user interface fields, Oracle Data Masking is certified with Oracle Fusion Applications.

The following entities are masked by Oracle Data Masking.

- Relational, transactional data across product families
- Dependent objects such as Intermedia Index or materialized views (MV)
- Empty tables such as those in schemas that are installed but not configured for use, are masked.

Oracle Fusion Applications provides masking definitions that specify only tables and columns that are possible candidates for masking.

The following table lists the masking template containing the masking definitions for each Oracle Fusion Applications offering.

<table>
<thead>
<tr>
<th>Offering</th>
<th>Masking Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Data Management</td>
<td>FUSION_CDM_VR1_Mask_Template.xml</td>
</tr>
<tr>
<td>Oracle Sales Cloud</td>
<td>FUSION_CRM_EXCEPT_CDM_TCA_VR1_Mask_Template.xml</td>
</tr>
<tr>
<td>Financials</td>
<td>FUSION_FIN_V1.0_Mask_Template.xml</td>
</tr>
<tr>
<td>Government Risk and Compliance</td>
<td>FUSION_GRC_VR1_Mask_Template.xml</td>
</tr>
<tr>
<td>Human Capital Management</td>
<td>FUSION_HCM_VR1_Mask_Template.xml</td>
</tr>
<tr>
<td>Procurement</td>
<td>FUSION_PRC_V1.0_Mask_Template.xml</td>
</tr>
<tr>
<td>Supply Chain Management</td>
<td>FUSION_SCM_VR1_Mask_Template.xml</td>
</tr>
<tr>
<td>Combined masking template for all product families</td>
<td>Combination_v1_ALL_Families.xml</td>
</tr>
</tbody>
</table>
The masking templates specify sensitive database tables and columns in Oracle Fusion Applications, and the data formats to be used to mask the columns. The masking templates provide examples as a starting point. They are not complete for all cases and can cause issues in how certain parts of the applications function.

Determine what data should be masked based on the needs of your enterprise. The purpose of the cloned data, what data you are storing, and so on, affects what masking to enable. You must balance the security of the masked test system against the usefulness of the masked test system to testers. You may need to accommodate specifics in your deployment such as customizations and the data semantics of flexfields to adequately mask all sensitive information.

---

**Caution**

As a security hardening guideline, change the sign on user IDs and passwords in the non-production database. Never use your production database credentials for sign on.

---

**Caution**

As a security hardening guideline, clone the data needed for the set of tests in question, or at least truncate any tables containing sensitive data that are not needed for the tests. Every piece of sensitive information that is cloned and not used, represents an unnecessary risk.
**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.

**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 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.

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, and payroll flows.

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.

URL
Abbreviation for uniform resource locator.

XML filter
A type of condition using XML to constrain the data secured by a data security policy.