Fusion Applications: Security Fundamentals

Duration: 3 Days

What you will learn

The course goes beyond the modification of the delivered predefined roles and gives a risk-based approach to security management. This course is centered on business-driven security objectives.
The training approach includes demonstrations, hands-on activities, discussions, and knowledge checks that will enable you to implement and administer security in your Oracle Fusion Applications deployment.

Learn To:

Attain security goals in an Oracle Fusion Applications deployment.
Administer security in Oracle Fusion Applications
Support implementations with specific security requirements

Audience

Administrator
Implementation Consultant
Security Administrators
Security Compliance Auditors
Security Compliance Professionals

Related Training

Suggested Prerequisites
Previous exposure to a Fusion Applications implementation

Course Objectives

Address the security administration tasks associated with bringing a new employee into the organization

Review function security provided by duty (application) roles

Review predefined data security policies, role template-generated data roles, and data roles determined by HCM security profiles

Identify the means by which users access functions and data, such as through menus, search, analytics, and tag clouds, and how these access methods are secured

Review the reference implementation to determine how to change job roles to more exactly represent the jobs within an enterprise

Recognize security controls as a priority, from role-based access to enforcement across the deployed technology stack

Understand which roles provide access to which activities

Use Oracle Functional Setup Manager (FSM) to enable offerings and options

Understand how access to the legal entity, ledger, and business unit enterprise structures is restricted

Identify the security administration and hardening tasks that mitigate risk to achieve confidentiality, integrity, and availability

Understand what security components and application strategies in Oracle Fusion Applications mitigate risk

Differentiate creation of implementation users created before enterprise setup from creation of regular application users after enterprise setup

Course Topics

Security Fundamentals Course Overview

Introduction to Oracle Fusion Applications

Functional Setup Manager Overview

Common Application Configuration Overview
Overview of InFusion Corporation
Defining Enterprise Structures
Manage Primary Ledgers
Ledger Security
Managing Business Units
Business Unit Security

Principal Security Goals
Areas of Risk
Components Ensuring Integrity
Hardening
Production User Roles
Identifying Orphaned, Ghost, or Inactive Accounts
Passwords and Credentials
Applications IDs
Managing Audit Policies

Managing Users
Implementation Users
How Initial Implementation Users Are Stored and Managed
Provisioning Initial Implementation Users with Roles
Application Users
How Application Users Are Created, Stored, and Managed
Comparing Applications Users to Initial Implementation Users
Creating Users

Importing Users

Managing Authorization
Security Reference Implementation
Role-Based Access Control Overview
Policies
Function Security
Data Security
Data Roles
Defining Data Security

Managing User Access Provisioning
Provisioning Roles to Users
Delegated Administration of Role Provisioning
Role Mappings Key Concepts
Role-Provisioning Strategies
Role Provisioning Rules
Role Provisioning Events

Managing Segregation of Duties
Predefined Segregation of Duties (SOD) Policies
Managing Application Access Controls
Detection
Reviewing Controls Monitors
Reviewing Detected Violations

Course Summary
Key Concepts
Key Terms
Security Reference Resources