Oracle® Fusion Middleware

Security Overview

11*g* Release 1 (11.1.1)

E12889-04

April 2011

Provides a high-level overview of security features and best practices in Oracle Fusion Middleware 11*g* Release 1.

ORACLE®

Oracle Fusion Middleware Security Overview, 11*g* Release 1 (11.1.1)

E12889-04

Primary Author: Vinaye Misra

Contents

List of Figures

List of Tables

Preface

This document provides a high level introduction to security in Oracle Fusion Middleware.

This preface contains these sections:

Audience

This document is intended for system architects, security administrators, and developers who want a road map of security in Oracle Fusion Middleware in 11*g* Release 1 (11.1.1).

After reading this document, you are able to:

- become familiar with the broad security landscape in Oracle Fusion Middleware, including the role and scope of security, and have basic knowledge about where to find specific information
- learn about Oracle Platform Security Services, which provide the foundation for a wide range of security features for administrators and developers
- understand common security tasks and where to go for more information on implementing security tasks

This document is designed primarily to introduce the security capabilities of Oracle Fusion Middleware in general and Oracle Platform Security Services in particular; details about the standard security features of Oracle WebLogic Server are not in the scope of this document.

For more details about security in Oracle WebLogic Server, and how to implement specific security features see the section titled "Related Documents" and the references provided in subsequent chapters of this document.

Document Organization

This document is organized as follows:

- Chapter 1, "Security in Oracle Fusion Middleware" explains the scope of security technologies in Oracle Fusion Middleware using an architecture diagram
- Chapter 2, "About Oracle Platform Security Services" introduces Oracle Platform Security Services and its key components, and explains the role and features of the different components
- Chapter 3, "Developing Secure Applications" explains how you can use Oracle Application Development Framework to develop secure applications
- Chapter 4, "Infrastructure Hardening" takes a high-level look at key aspects of infrastructure security
- Chapter 5, "Common Security Scenarios and Tasks" describes the most common security tasks, and where to find information about performing those tasks

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/support/contact.html` or visit `http://www.oracle.com/accessibility/support.html` if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle 11*g* Release 1 (11.1.1) documentation set:

- *Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server*
- *Oracle Fusion Middleware Application Security Guide*
- *Oracle Fusion Middleware Administrator's Guide*

- *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*

Chapter 3, "Common Security Tasks," provides additional references for specific tasks.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in This Guide?

This preface introduces the new and changed administrative security features in Oracle Fusion Middleware, and provides pointers to additional information.

Note: This preface lists the new features that are highlighted in this document. For a complete list of all new and changed security features, see:

- What's New in This Guide in the *Oracle Fusion Middleware Application Security Guide*
- The What's New preface of Oracle Identity Management component guides

New Content for Oracle Fusion Middleware 11*g* Release 1 (11.1.1.5)

This document introduces the following new and changed security and identity management features in Oracle Fusion Middleware 11g Release 1 (11.1.1.5):

- Oracle Entitlements Server

  For details, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*.

- Audit loader for Java SE applications.

  For details, see Section 2.3.8, "Auditing"

- Oracle Security Token Service

This document includes the following new content and revisions:

- A discussion of audit reports for Oracle Identity Management components.

  For details, see Section 5.3.6, "References for Auditing".

- Common tasks related to fine-grained access control.

  For details, see Section 5.3.4, "References for Authorization".

New Content for Oracle Fusion Middleware 11*g* Release 1 (11.1.1.4)

This document introduces the following new security and identity management features in Oracle Fusion Middleware 11g Release 1 (11.1.1.4):

- Support for IBM WebSphere application server. See the *Oracle Fusion Middleware Third-Party Application Server Guide* for more information.

- Support for database security stores.

  For details, see the *Oracle Fusion Middleware Application Security Guide*.

- The Oracle SSL Automation Tool, which replaces manual procedures and simplifies SSL configuration. See the *Oracle Fusion Middleware Administrator's Guide*.

1

Security in Oracle Fusion Middleware

This chapter provides a survey of security capabilities in Oracle Fusion Middleware and a road map for system administrators and application developers. It contains these topics:

1.1 Terminology

We start by defining some common terms that are used in this document and throughout the related documents listed in the preface.

Some industry standards, such as SAML, are included for their relevance to later discussion. The list is not intended to be comprehensive.

Application Life cycle

An application can be provided by Oracle or by a third-party vendor, or it can be developed in-house. In all cases, applications are designed to run in an application server environment and to take advantage of Oracle Fusion Middleware features and capabilities.

The typical life cycle of an application includes these phases:

- development
- deployment
- Migration (Test to Production)
- Upgrade (for example, from Release 10.1.x to Release 11*g*)
- ongoing maintenance tasks (for example, patching) in a production environment.

Security is an integral part of the application life cycle, although the scope and implementation details may vary.

For example, at development time user credentials can simply be stored in a file, whereas a deployed application is generally secured with an identity management solution using an LDAP directory at the back-end.

Audit

Auditing is a process that measures accountability. In the Identity and Access Management space, auditing provides reports and the data that shows who accessed what resources and when.

Authentication

Authentication verifies that the user is who she claims to be. A user's identity is verified through the credentials presented by that user, such as:

1. something one has, for example, credentials issued by a trusted authority such as a passport (real world) or a smart card (IT world),
2. something one knows, for example a shared secret such as a password,
3. something one is, for example, biometric information

A combination of several types of credentials is referred to as "strong" authentication; an example is the use of an ATM card (something one has) with a PIN or password (something one knows).

Authorization

Also known as access control, authorization is designed to grant access to specific resources based on an authenticated user's entitlements. Entitlements are defined by one or several attributes. An attribute is the property, characteristic, or role of a user; for example, if "Raj" is the user, "software engineer" is the attribute (or role).

Authorization is based on the enforcement of access policies; for example, if Raj is assigned the software engineer role, he can access specific application code.

Credential Store

A credential store is a service that you can use to store passwords to external applications and systems such as databases or LDAP directories.

In Oracle Fusion Middleware 11*g* Release 1 (11.1.1), the credential store is either file-based (Oracle wallet) or an LDAP-based repository for storing credentials such as passwords.

Development Phase

The development phase is the first stage in the life cycle of an application. During this phase, developers code the application logic and presentation layers.

Using Oracle Application Development Framework (Oracle ADF), developers can make use of Oracle ADF's built-in support for a range of security features.

For details, see:

- Section 3, "Developing Secure Applications"
- Enabling ADF Security in a Fusion Web Application in the *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*

Deployment Phase

The deployment phase is the second stage in the life cycle of an application. During this phase, administrators package the application and deploy it to the target environment (for example, an application server) to enable end user access.

In the deployment phase, administrators typically perform application role-to-enterprise group mappings. For more information, see

- Deploying JavaEE and Oracle ADF Applications with Fusion Middleware Control
- Section 5.2, "Summary of Common Security Tasks".

Identity Store

An identity store is a trusted store where user identities (users and groups) are kept.

In Oracle Fusion Middleware 11*g* Release 1 (11.1.1), the default identity store is an embedded LDAP store maintained in the Oracle WebLogic Server process suitable for testing and small-scale deployments only. Enterprise LDAP servers (Oracle Internet Directory and third-party LDAP directories) are also supported.

See Section 2.3.1, "Authentication" for related information.

Infrastructure Hardening

The infrastructure refers to the full range of system software required to deploy an application. Infrastructure hardening is the process of applying security to each component of the infrastructure, including web servers, application servers, identity and access management solutions, and database systems. Infrastructure hardening is the basis for end-to-end security across the multiple infrastructure components involved in a transaction.

Note: In the context of securing Oracle WebLogic Server, this task is referred to as "lockdown." However, in the broader context of Oracle Fusion Middleware, it is referred to as infrastructure hardening.

See Also: The WebLogic Security Service provides a powerful and flexible set of software tools for securing the subsystems and applications that run on a server instance. For details, see *Oracle Fusion Middleware Developing Web Applications, Servlets, and JSPs for Oracle WebLogic Server*

Java Authentication and Authorization Service (JAAS)

JAAS can be used for two purposes:

- for authentication of users, to reliably and securely determine who is currently executing Java code, regardless of whether the code is running as an application, an applet, a bean, or a servlet; and
- for authorization of users to ensure they have the access control rights (permissions) required to do the actions performed.

For details, see the Java Authentication and Authorization Service (JAAS) Reference Guide at:

`http://java.sun.com/javase/6/docs/technotes/guides/security//jaas/JAASRefGuide.html`

Java Component

A Java component is a peer of a system component, and is managed by the application server container. Examples include Oracle SOA Suite and Oracle Identity Federation.

Keystore

Objects necessary for SSL communication, including private keys, digital certificates, and trusted CA certificates are stored in keystores.

Oracle Fusion Middleware provides two types of keystores for keys and certificates:

- JKS-based keystore and truststore, the default JDK implementation of Java keystores provided by Sun Microsystems. JKS keystores are used for Oracle Virtual Directory and other products.

- Oracle wallet, a container for PKCS#12-based credentials. Oracle wallets are used for Oracle Internet Directory and other products.

For more information, see Section 4.2, "Keystores".

Oracle Application Development Framework (ADF)

Oracle Application Development Framework (Oracle ADF) is an innovative, comprehensive Java EE development framework that is directly supported and enabled by the Oracle JDeveloper 11g development environment.

Oracle ADF simplifies Java EE development by minimizing the code that implements the application's infrastructure, allowing the users to focus on the features of the actual application. Oracle ADF provides these infrastructure implementations as part of the framework. To recognize a set of run-time services is not enough, Oracle ADF is also focused on the development experience to provide a visual and declarative approach to Java EE development through the Oracle JDeveloper 11g development tool.

Oracle ADF is based upon Oracle Platform Security Services.

Oracle Access Manager (OAM)

Oracle Access Manager is available for both 10*g* and 11*g* releases:

- Oracle Access Manager 10*g* provides a full range of identity administration and security functions that include Web single sign-on; user self-service and self-registration; sophisticated workflow functionality; auditing and access reporting; policy management; dynamic group management; and delegated administration.
- Oracle Access Manager 11*g* provides a full range of web perimeter security functions that include Web single sign-on; authentication and authorization; identity assertion; policy administration; and auditing.

  Oracle Access Manager 11*g* differs from Oracle Access Manager 10*g* in that the identity administration features, including user self-service and self registration, sophisticated workflow functionality, dynamic group management, and delegated identity administration have been transferred to Oracle Identity Manager 11*g*. At the same time, Oracle Access Manager 11*g* provides access control to Oracle Identity Manager 11*g*.

  See Also: "Oracle Identity Manager".

Oracle Adaptive Access Manager (OAAM)

Rapid growth in online applications and services has brought increasing sophistication of internet fraud. Threats from Phishing, Pharming, Trojans, Key Logging, and Proxy Attacks, combined with regulations and mandates (such as FFIEC, HIPAA, PCI) governing online data privacy, place online security at a premium.

Oracle Adaptive Access Manager provides superior protection for businesses and their customers through strong yet easy-to-deploy authentication strengthening, multifactor authentication and proactive, real-time fraud prevention.

Oracle Directory Server Enterprise Edition

Formerly SUN Directory Server Enterprise Edition, Oracle Directory Server Enterprise Edition is the best known directory server with proven large deployments in carrier and enterprise environments. It is also the most supported directory by ISVs, so it is ideal for heterogeneous environments. ODSEE provides a core directory service with

embedded database, directory proxy, Active Directory (AD) synchronization and a Web administration console.

See Also: "Oracle Internet Directory"

Oracle Enterprise Manager Fusion Middleware Control

Fusion Middleware Control is a JMX-based GUI management tool provided as part of Oracle Enterprise Manager.

Oracle Entitlements Server

Oracle Entitlements Server is a fine-grained entitlements management solution that externalizes and centralizes administration of enterprise entitlements, simplifies authorization policies, and enforces security decisions in distributed, heterogeneous applications.

Oracle Entitlements Server secures access to application resources and software components (such as URLs, EJBs, and JSPs) and to arbitrary business objects (such as customer accounts or patient records). Oracle Entitlements Server policies specify which users, groups, and roles can access application resources, allowing those roles to be dynamically resolved at run-time.

Oracle Entitlements Server can also evaluate specialized attributes to make more granular access control decisions through a unique, flexible architecture called Security Modules. The server's standalone administration service manages and distributes complex entitlements policies to policy decision and enforcement points. Security modules may run in a centralized mode or they can be embedded within an application, ensuring maximum flexibility and high performance authorizations for business critical applications.

Oracle Identity Analytics

Oracle Identity Analytics (formerly Sun Role Manager) enables enterprises to engineer and manage roles and automate critical identity-based controls. Its key features include a central repository of identity, access and audit data, optimized for complex analytical queries; automated attestation processes providing a 360-degree view of users' access; segregation of duties (SoD) enforcement; role lifecycle management; and various compliance and operational dashboards.

Oracle Identity Federation

Oracle Identity Federation is an industry-leading federation solution providing a self-contained and flexible multi-protocol federation server that can be rapidly deployed with your existing identity and access management systems. Support for leading standards-based protocols ensures interoperability to share identities across vendors, customers, and business partners without the increased costs of managing, maintaining, and administering additional identities and credentials.

Oracle Identity Manager

Oracle Identity Manager is a best-in-class user provisioning and administration solution that automates the process of adding, updating, and deleting user accounts from applications and directories; and improves regulatory compliance by providing granular reports and attestation support to report and certify user access.

Oracle Internet Directory

Oracle Internet Directory is an LDAP v3 compliant directory with meta-directory capabilities. It is built on the industry leading Oracle database and is fully integrated

into Oracle Fusion Middleware and Oracle Applications. Thus, it is ideally suited for Oracle environments or enterprises with Oracle database expertise.

Oracle Internet Directory provides security at every level from data in transit to storage and backups. In addition to LDAP security, it leverages Oracle database security features like Database Vault and Transparent Data Encryption. Database Vault enables separation of duty (SOD) while Transparent Data Encryption secures data in storage and backup.

See Also: "Oracle Directory Server Enterprise Edition"

Oracle Platform Security Services (OPSS)

Oracle Platform Security Services (OPSS) provides enterprise product development teams, systems integrators (SIs), and independent software vendors (ISVs) with a standards-based, portable, integrated, enterprise-grade security framework for Java Standard Edition (Java SE) and Java Enterprise Edition (Java EE) applications.

OPSS provides an abstraction layer in the form of standards-based application programming interfaces (APIs) that insulate developers from security and identity management implementation details. In-house developed applications, third-party applications, and integrated applications all benefit from the same uniform security, identity management, and audit services across the enterprise.

When they leverage OPSS, developers do not have to know the details of cryptographic key management or interfaces with user repositories and other identity management infrastructures.

Oracle Security Token Service

Oracle Security Token Service brokers trust between a Web Service Consumer (WSC) and a Web Service Provider (WSP) and provides security token lifecycle management services to providers and consumers.

Oracle Security Token Service is compliant and co-exists with Oracle Access Manager (using Oracle Access Manager as the primary authenticator for Web clients requesting tokens).

Oracle Virtual Directory

Oracle Virtual Directory provides identity aggregation and virtualization without synchronization. It is not LDAP storage, but rather, a virtualization service. Key features include a single interface for identity, an LDAP interface for non-LDAP data including databases and Web services, data transformation features, and application-specific views of data.

For customers who also need directory storage, Oracle Virtual Directory shares a unified administration and management system with Oracle Internet Directory.

Oracle Web Services Manager

Oracle Web Services Manager is a comprehensive solution for adding policy-driven best practices to all your existing or new Web services and provides the key security and management capabilities necessary to deploy Service-Oriented Architectures across your line-of-business applications.

Oracle Web Services Manager is Oracle Fusion Middleware's policy model, based on WS-Policy. Oracle Web Services Manager provides security to many Oracle Fusion Middleware components such as Oracle WebCenter, Oracle ADF, and OSB.

Oracle Web Services Manager allows IT management to centrally define policies that govern Web services operations (such as access policy, logging policy, and load

balancing), then wrap these policies around Web services without needing to modify those services.

Oracle Web Services Manager collects monitoring statistics to ensure quality of service, uptime, and security threats and displays them in a Web dashboard.

Oracle Wallet

An Oracle wallet is a container that stores credentials such as certificates, trusted certificates, certificate requests, and private keys. You can store Oracle wallets on the file system or in LDAP directories such as Oracle Internet Directory. Oracle wallets can be auto-login or password-protected wallets.

You use an Oracle wallet for the following components:

- Oracle HTTP Server
- Oracle Web Cache
- Oracle Internet Directory

Partner Applications

A partner application is an Oracle Application Server-based application or a non-Oracle application that delegates the authentication function to the OracleAS SSO (OSSO) server. A partner application is responsible for determining whether a user authenticated by OSSO is authorized to use the application. Examples of partner applications include Oracle Portal, Oracle Discoverer, and Oracle Delegated Administration Services.

> **Note:** Oracle recommends using Oracle Access Manager 11g. For details, see Introduction to Oracle Access Manager 11g SSO in the *Oracle Fusion Middleware Application Security Guide*.

Security Assertions Markup Language (SAML)

Security Assertions Markup Language (SAML) is an XML-based framework for exchanging security information over the Internet. SAML enables the exchange of authentication and authorization information between various security services systems that otherwise would not be able to interoperate.

Single Sign-On

Single sign-on enables a user to authenticate once and gain access to several applications without the need to re-authenticate.

System Component

A system component is a manageable process that is not Oracle WebLogic Server. Examples include Oracle HTTP Server and Oracle Internet Directory.

Web Services Security

Web services security includes authentication and authorization (described above), confidentiality and privacy (keeping information secret), and integrity / non repudiation (making sure that a message remains unaltered during transit by having an authority digitally sign that message; a digital signature also validates the sender and provides a time stamp ensuring that a transaction cannot be later repudiated by either the sender or the receiver). Web services security requirements are supported by industry standards both at the transport level (Secure Socket Layer) and at the

application level relying on XML frameworks, for example XML encryption, XML signature, and Security Assertion Markup Language (SAML).

eXtensible Access Control Markup Language (XACML)

XACML is a declarative standard for languages that specify both access control policy and access control request/response requirements.

1.2 Scope of Security in Oracle Fusion Middleware

By Oracle Fusion Middleware security, we mean the full range of security options available to applications throughout their life cycle in 11*g* Release 1 (11.1.1). At the outset it is important to note that, beginning with this release, Oracle WebLogic Server is the application server for Oracle Fusion Middleware. Existing users can continue to use the security facilities provided by Oracle WebLogic Server, using the same configuration tools as before.

Oracle WebLogic Server security is unchanged in 11*g* Release 1 (11.1.1) and customers can use existing Oracle WebLogic Server tools for managing base container/JavaEE security.

> **See Also:** Chapter 5, "Common Security Scenarios and Tasks" for more information about the different security options in Oracle Fusion Middleware.

1.2.1 About Authentication and Single Sign-On

Oracle Fusion Middleware supports a range of authentication and single sign-on options, including:

- Authentication Providers

  An authentication provider allows Oracle WebLogic Server to establish trust by validating a user.

- Identity Assertion Providers

  An identity assertion provider is a type of authentication provider that handles perimeter-based authentication and multiple security protocols and token types.

- Identity Stores

  See "Identity Store" for information.

- Support for 10*g* Oracle Single Sign-On and 10*g* Oracle Access Manager.

  > **Note:** Oracle Access Manager is the preferred solution. For more information, see Section 5.1, "Single Sign-On".

  Oracle WebLogic Server contains authentication providers for both of these products.

1.2.2 About Oracle Platform Security Services

As noted earlier (see Section 1.1, "Terminology"), Oracle Platform Security Services (OPSS) provides a standards-based, portable, integrated, enterprise-grade security framework for Java Standard Edition (Java SE) and Java Enterprise Edition (Java EE) applications.

OPSS provides security services to both Oracle WebLogic Server and such Oracle components as:

- Oracle SOA Suite
- Oracle WebCenter
- Oracle Entitlement Server
- Oracle Web Services Manager

OPSS incorporates the Security Service Provider Interfaces for Oracle WebLogic Server, and Oracle's 10*g* security framework, referred to as Java Platform Security (JPS).

For details, see Chapter 2, "About Oracle Platform Security Services".

1.2.3 About Security for Oracle SOA Suite

At the transport level, Oracle SOA Suite relies primarily on the security features of Oracle WebLogic Server and Oracle Fusion Middleware. For example, you enable Secure Socket Layer (SSL) on Oracle SOA Suite connections into Oracle WebLogic Server by using the Oracle WebLogic Server Administration Console to configure listeners. At the message level, Oracle SOA Suite relies on Oracle Web Services Manager.

In addition, here are some suite-specific aspects of security:

- Securing SOA Composites
  - Two-way SSL
  - SSL between Oracle SOA Suite and Oracle HTTP Server
  - automatic authentication when accessing a second Oracle BPM Worklist from a first Oracle BPM Worklist in Security Assertion Markup Language (SAML) single sign-on environments
  - automatic authentication of Oracle BPM Worklist users in Windows native authentication environment through Kerberos
- Securing Oracle Business Activity Monitoring
  - Credential Mapping
  - Oracle BAM User Permissions
  - Oracle Internet Directory with Oracle BAM
- Securing Oracle User Messaging Service
  - Secure storage of sensitive driver properties like passwords in the credential store
  - transport-level security using SSL

For details, see the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

1.2.4 About Security for Oracle WebCenter

At the message level, Oracle WebCenter relies on Oracle Web Services Manager for security.

Besides the application layer, Oracle WebCenter supports four security layers:

- The WebCenter Spaces application supports:
  - Application role management and privilege mapping
  - Self-registration
  - Group Space security management
  - Account and password management
- The WebCenter Security Framework supports:
  - Service Security Extension Framework
  - Permission- and Role-mapping-based authorization
  - External applications and credential mapping
- ADF Security supports:
  - Page and task flow authorization
  - Secure connection management
  - Credential mapping APIs
- Oracle Platform Security Services (OPSS) supports:
  - Anonymous-role and Authenticated-role support
  - Identity store, policy store, and credential store
  - Identity Management Services
  - Oracle Web Services Manager Security

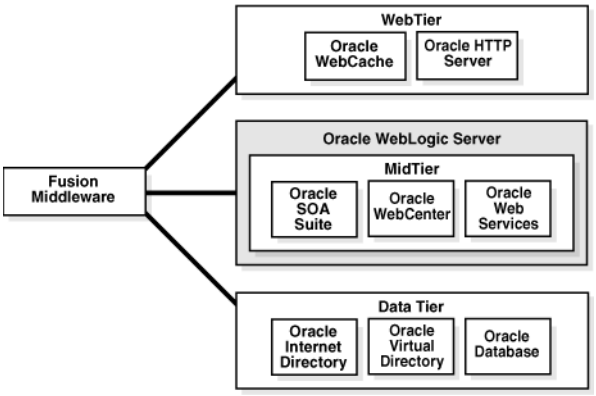
For details, see Managing Security in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter*.

1.3 Oracle Fusion Middleware and the Three-Tier Architecture

Security can be defined as controlled access to the Oracle Fusion Middleware infrastructure and to enterprise applications built upon that infrastructure.

Figure 1–1 shows how Oracle Fusion Middleware supports the classic three-tier enterprise environment:

Figure 1–1 Oracle Fusion Middleware and the Three-Tier Model



In this model:

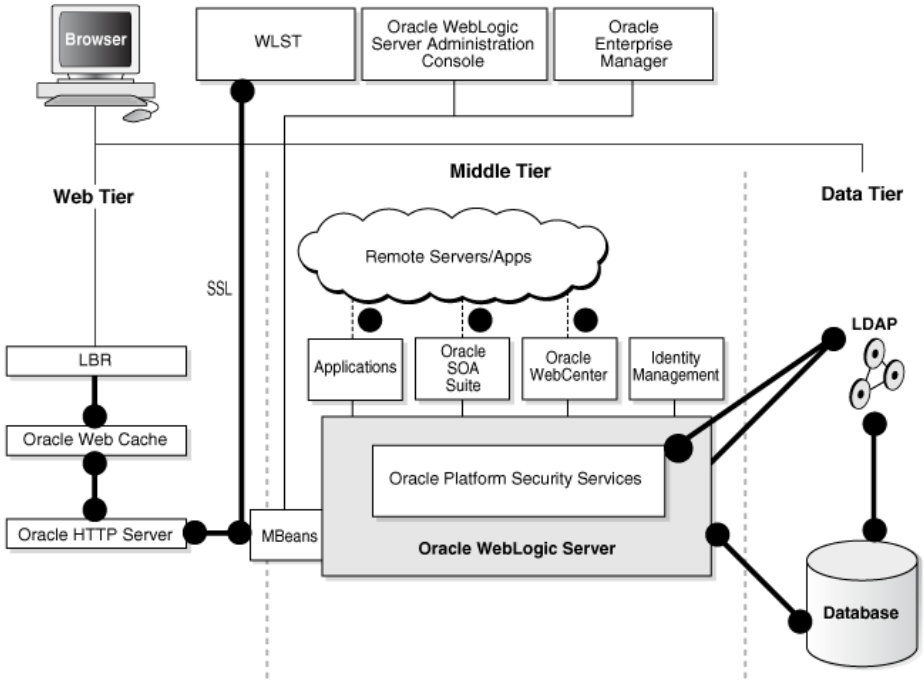
- The Web tier consists of components like WebCache and Oracle HTTP Server, which protect resources and control access to applications.
- The Middle tier runs Oracle WebLogic Server, which hosts the security Service Provider Interfaces (SPIs) and APIs. Oracle Fusion Middleware components such as Oracle SOA Suite, Oracle WebCenter, and Oracle Web Services Manager operate in the middle tier.

  See Also : Section 2.1.2, "How Applications Can Use Oracle Platform Security Services" for a description of the SPI model.

- The data tier is the repository for LDAP directories and databases, such as Oracle Internet Directory, Oracle Virtual Directory, and Oracle Database.

The following diagram is a high-level overview of the major elements of security in Oracle Fusion Middleware:

Figure 1–2 Security in Oracle Fusion Middleware



This figure shows the elements of security in Oracle Fusion Middleware: the Web tier on the left contains load balancers and other components outside the firewall; the middle tier hosts Oracle WebLogic Server and its applications; and on the right, the Data tier contains databases and directories. Different administration tools are shown at the top of the figure.

Key elements of this architecture are as follows:

- Fusion Middleware Control, GUI-based administration tool for Oracle Fusion Middleware. You use Fusion Middleware Control to configure, manage and monitor components and applications, and to implement security for these components:
  - Oracle HTTP Server
  - Oracle Web Cache

  - Oracle Internet Directory
  - Oracle Virtual Directory
- Oracle WebLogic Server is the application server for Oracle Fusion Middleware components such as Oracle SOA Suite, Oracle Identity Management, Oracle WebCenter, and applications developed by customers, system integrators, and third-party vendors.
- The vertical broken lines represent firewalls
- The circles represents listeners that can be SSL-enabled for secure communication

  For details, see Chapter 4, "Infrastructure Hardening".

1.3.1 Tools for Managing Oracle Fusion Middleware

Oracle Fusion Middleware contains these graphical and command-line run-time tools:

- Oracle WebLogic Server Administration Console enables you to configure Oracle WebLogic Server domains and JavaEE applications running on the server
- Fusion Middleware Control enables you to configure Oracle applications running on the server, and to leverage security features that rely on the OPSS APIs.
- The Oracle WebLogic Scripting Tool (`WLST`) is a command-line scripting environment that you can use to create, manage, and monitor WebLogic Server domains, and administer Oracle Fusion Middleware security features
- Oracle Business Intelligence Publisher enables you to view audit reports

2

About Oracle Platform Security Services

Oracle Platform Security Services comprises Oracle WebLogic Server's internal security framework and Oracle's security framework (referred to as Oracle Platform Security). OPSS delivers security as a service within a comprehensive, standards-based security framework.

This chapter contains these topics:

- Overview of Oracle Platform Security Services (OPSS)
- Oracle Platform Security Services Architecture
- Overview of Services

Read this chapter to understand:

- what role OPSS plays in Oracle Fusion Middleware architecture
- the components of OPSS
- where to use different OPSS features
- where to obtain more details about OPSS

For details, see Introduction to Oracle Platform Security Services in the *Oracle Fusion Middleware Application Security Guide*.

2.1 Overview of Oracle Platform Security Services (OPSS)

Oracle Platform Security Services (OPSS) provides enterprise product development teams, systems integrators (SIs), and independent software vendors (ISVs) with a standards-based, portable, integrated, enterprise-grade security framework for Java Standard Edition (Java SE) and Java Enterprise Edition (Java EE) applications.

OPSS provides an abstraction layer in the form of standards-based application programming interfaces (APIs) that insulate developers from security and identity management implementation details. With OPSS, developers do not have to know the details of cryptographic key management or interfaces with user repositories and other identity management infrastructures. By leveraging OPSS, in-house developed applications, third-party applications, and integrated applications all benefit from the same uniform security, identity management, and audit services across the enterprise.

2.1.1 Oracle Platform Security Services in Oracle Fusion Middleware

Here is a list of Oracle Fusion Middleware components that use Oracle Platform Security Services:

- Oracle WebLogic Server

- Oracle Entitlements Server
- Oracle WebCenter
- Oracle SOA Suite
- Oracle Identity Management, including:
  - Oracle Internet Directory
  - Oracle Virtual Directory
  - Oracle Identity Federation
- Oracle Web Services Manager
- Oracle Application Development Framework (ADF)

2.1.2 How Applications Can Use Oracle Platform Security Services

By leveraging Oracle Platform Security Services systems integrators (SIs), and independent software vendors (ISVs) can build their applications and products using the same security building blocks that are used by Oracle products.

Key features of OPSS include:

- Extensive security services:
  - Authentication
  - Authorization
  - Credential Store Framework
  - User and Role APIs
  - Policy Management APIs
  - Single Sign-On
  - Identity Assertion
  - Auditing
  - Oracle Security Developer Tools, a comprehensive security API library

  More information about each service is available in Section 2.3, "Overview of Services".
- Service provider model

  Unlike the case with other application servers, OPSS not only provides security services for the application server, but also enables applications to leverage the same services to seamlessly implement authentication, authorization, and other security features available to Oracle system components.
- Support for Enterprise Standards

  The framework supports key standards including:
  - Java EE
  - SAML
  - XACML
  - JACC
  - JAAS

See Also: Section 1.1, "Terminology" for information about these standards.

- Support for Windows Native Authentication
- Support for SPNEGO
- Portability

  OPSS is a portable framework:

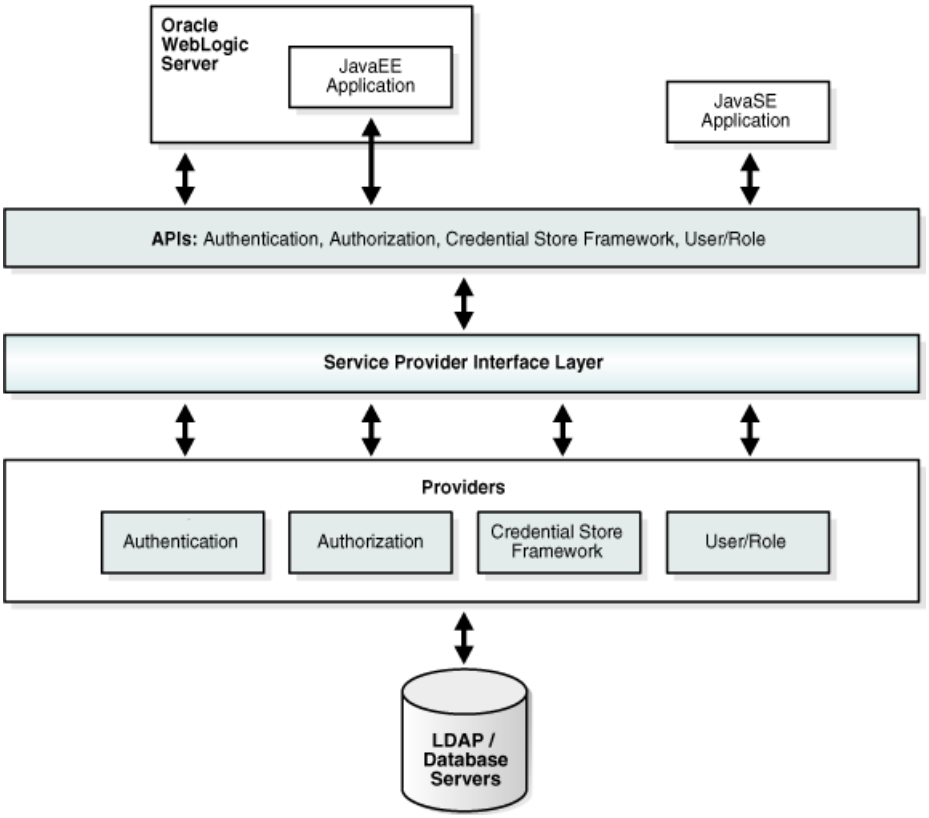
  - you can build enterprise JavaEE and standalone JavaSE applications in a consistent security framework and ensure a consistent security implementation
  - the service provider interface (SPI) model enables you to implement custom security providers relying on a standards-based security platform
  - the security framework is not tied to a specific application server
- Ease of development
- Available on both JavaEE and JavaSE platforms
- Integrated with various back-end data stores (LDAP, RDBMS, custom)

Since OPSS provides the building blocks for securing applications, it simplifies development and allows application developers to focus on solving business problems while relying on OPSS to provide security consistently, in a portable manner, across the enterprise.

2.2 Oracle Platform Security Services Architecture

Figure 2–1 shows the environment and building blocks of OPSS and the roles they play in providing security services.

Figure 2–1 Oracle Platform Security Services Architecture



This figure depicts the various security components as layers. The uppermost layer consists of Oracle WebLogic Server and the components and Java applications running on the server; below this is the API layer consisting of Authentication, Authorization, CSF, and User and Role APIs, followed by the Service Provider Interface (SPI) layer and the service providers for authentication, authorization, and others. The final and bottom layer consists of repositories including LDAP and database servers.

Oracle Platform Security Services

Oracle Platform Security Services (OPSS) is both a security framework exposing security services and APIs, and a platform offering concrete implementation of security services. It includes these elements:

- Common Security Services (CSS), the internal security framework on which Oracle WebLogic Server is based

  This framework provides security to Oracle WebLogic Server, Oracle Entitlements Server, and many other products that previously ran on the application server, and continue to do so in 11*g* Release 1 (11.1.1)

- Oracle Platform Services

  This framework provides security to Oracle applications, for example, Oracle Application Development Framework (ADF), Oracle WebCenter, Oracle SOA Suite, Oracle Web Services Manager (OWSM) and other products that previously ran on Oracle Application Server, and continues to support these products in 11*g* Release 1 (11.1.1)

- User and Role APIs
- Oracle Fusion Middleware Audit Framework

This framework provides auditing capabilities for components.

- Oracle Security Developer Tools
- Identity Governance Framework (IGF).

  This framework enables you to address governance of identity related information across enterprise IT systems. For information about IGF and the ArisID implementation, see:

  http://www.oracle.com/technology/tech/standards/idm/igf/index.html

For details, see OPSS Architecture Overview in the *Oracle Fusion Middleware Application Security Guide*.

Oracle Platform Security Services APIs

OPSS APIs provide a full range of security capabilities:

- authentication,

  authorization,
- fine-grained authorization,
- auditing

and other services.

For more information, see:

- Section 2.3, "Overview of Services"
- Overview of Developing Secure Applications with Oracle Platform Security Services in the *Oracle Fusion Middleware Application Security Guide*.

Third-Party Application Servers

OPSS provides support for third-party application servers. For details, see *Oracle Fusion Middleware Third-Party Application Server Guide*.

2.3 Overview of Services

Table 2–1 lists the different services available in this release.

Table 2–1 Oracle Fusion Middleware Security Services

Service	Data Store	More Information
Authentication	Identity Store	Understanding Identities, Policies, and Credentials in the *Oracle Fusion Middleware Application Security Guide*
Authorization	Policy Store	Understanding Identities, Policies, and Credentials in the *Oracle Fusion Middleware Application Security Guide*
Credential Store Framework	Credential Store	Understanding Identities, Policies, and Credentials in the *Oracle Fusion Middleware Application Security Guide*
Users and Roles	Identity Store	Understanding Users and Roles in the *Oracle Fusion Middleware Application Security Guide*
Policy Management	Policy Store	Policy Store Basics in the *Oracle Fusion Middleware Application Security Guide*

Table 2–1 (Cont.) Oracle Fusion Middleware Security Services

Service	Data Store	More Information
Single Sign-On	Identity Store	Configuring Single Sign-On in Oracle Fusion Middleware in the *Oracle Fusion Middleware Application Security Guide*
Identity Assertion	Identity Store	Identity Assertion Providers in *Oracle Fusion Middleware Developing Security Providers for Oracle WebLogic Server*
SSL	--	SSL Configuration in Oracle Fusion Middleware in the *Oracle Fusion Middleware Administrator's Guide*
Auditing	Audit Store	*Oracle Fusion Middleware Application Security Guide*
Security Developer Toolkit	--	*Oracle Fusion Middleware Reference for Oracle Security Developer Tools*
Services in Oracle WebLogic Server	--	*Oracle Fusion Middleware Securing Oracle WebLogic Server*

The remainder of this section provides a survey of each service.

See Also: For more information about securing Oracle WebLogic Server, see:

- *Oracle Fusion Middleware Securing Oracle WebLogic Server*
- *Oracle Fusion Middleware Programming Security for Oracle WebLogic Server*

2.3.1 Authentication

In Oracle Fusion Middleware, users are authenticated against an identity store, which is a trusted source of user identities. The authentication process can make use of username-password combinations, tickets, and public key certificates. Credentials supplied by a user are verified against the store during authentication and used to grant the user access to application functions.

The identity store is implemented through Oracle WebLogic Server LDAP authenticators.

Out-of-the-box, Oracle WebLogic Server stores user identities in an embedded LDAP repository. In a deployed production environment, Oracle recommends using an LDAP directory as the identity store. Oracle Fusion Middleware 11gR1 supports a wide array of LDAP servers as identity store including:

- Oracle Internet Directory
- Oracle Virtual Directory
- Sun Java System Directory Server
- Microsoft Active Directory
- Open LDAP
- Novell eDirectory
- generic

OPSS employs WebLogic authentication providers, components that validate user credentials or system processes based on a user name-password combination or a

digital certificate. Oracle WebLogic Server supports the aggregation of authentication providers, so that multiple stores can be used during verification.

For details, see:

- Authentication Basics in the *Oracle Fusion Middleware Application Security Guide*.
- *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

2.3.1.1 Authentication Recommendations

A site's authentication needs depend on the phases of the application life cycle:

- Development Phase – when an application is being developed
- Staging Phase - where the application is validated for production readiness, and
- Production Phase - when the application is ultimately deployed and utilized by end-users.

Authentication during the application development phase typically involves using a login module and by the native testing of user identity and policies. Additionally, some developers may also package application policies as part of the application archive (`WAR`) before handing it off for deployment in staging and production environments.

Authentication in the Development Phase

Oracle JDeveloper 11gR1, a component of Oracle Fusion Middleware, provides a unified application development environment.

Any application developed with JDeveloper can be tested against Oracle WebLogic Server's embedded LDAP server. The embedded LDAP server is the default security provider store for WebLogic authentication, authorization, credential mapping, and role mapping providers.

Oracle recommends using the embedded LDAP server to test application authentication during development.

> **See Also:** Managing the Embedded LDAP Server in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

> **See Also:** Packaging a JavaEE Application Manually in the *Oracle Fusion Middleware Application Security Guide*.

Single Sign-On Solutions in Staging and Production Phases

Once an application is deployed, the choice of an authentication mechanism depends on the configuration of the Oracle Weblogic Server domain in the staging or production environments. The configuration can take the following forms:

- Using Oracle Single Sign-On for all or specific applications that are deployed across multiple domains
- Using Oracle Access Manager for all applications or specific applications that are deployed across multiple domains
- Using a third-party single sign-on solution for all applications or specific applications that are deployed across multiple domains
- Using Windows Native Authentication for applications deployed on Windows platforms
- Using a federation approach

See Also:

- Configuring Single Sign-On in Oracle Fusion Middleware in the *Oracle Fusion Middleware Application Security Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
- *Oracle Access Manager Identity and Common Administration Guide*

2.3.2 Authorization

Authorization refers to access control by the use of policies. The authorization process enforces policies, determines what types of activities one can do, or what types of services one can access. Oracle Platform Security Services supports two authorization models for JavaEE and ADF applications.

- JavaEE Role-based Access Control
- Oracle ADF Security

Authorization based on JavaEE Role-based Access Control

For Java EE applications, Oracle Fusion Middleware supports JavaEE's role-based access control (RBAC) model, which has logical roles and physical roles. Logical roles are role names used in application code. Physical roles exist in an identity store. During application deployment, the administrator maps the logical role to a physical role.

Authorization based on Oracle ADF

Oracle Platform Security Services supports a fine-grained, permission-based authorization model which protects a resource using JAAS-based `checkPermission` calls.

See Using the method checkPermission in the *Oracle Fusion Middleware Application Security Guide* for details.

Leveraged by Oracle Application Development Framework and Oracle WebCenter applications, this model provides a fine-grained authorization capability; for example, you can apply authorization checks separately to individual ADF regions of the application.

Authorization in the Development Phase

Oracle JDeveloper enables you to choose between the Java EE and ADF authorization models.

The ADF authorization model provides an easy-to-use wizard.

Oracle recommends using representative data from the production environment as much as possible during these tests.

Documented procedures address the following Java EE authorization topics:

- How to configure the Java EE security model in Oracle Jdeveloper using embedded LDAP
- How to configure security in deployment descriptors by granting resource (URL or EJB method) to a logical role in the `web.xml` and `ejb-jar.xml` files

Documented procedures address the following ADF authorization topics:.

- How to configure the ADF security model using the ADF security wizard in Oracle JDeveloper
- How to configure fine-grained security for each region of the ADF page
- How to grant selective page elements and define the actions for those elements corresponding to a logical role

For details, see:

- *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*
- Policy Store Basics in the *Oracle Fusion Middleware Application Security Guide*.

Authorization in the Staging/Deployment Phases

As a rule, developers are not aware of the enterprise roles (groups) that exist in an identity store and are thus unaware of the authorization policies to apply. Authorization policies are typically implemented during deployment into a production environment.

The following documented procedures help the domain administrator during application deployments:

- How to map the logical roles used in an application to the enterprise groups that exist in an identity store using the management tools that ship with Oracle Fusion Middleware
- How to choose application-specific policies that must migrate to the domain policy store
- Over time, as the application's security needs evolve, how to use management tools like Oracle Fusion Middleware Control and WLST to make appropriate changes to the application's policies
- In an environment that uses Oracle Single Sign-On with LDAP, how to configure these single sign-on environments to use the same user population for both authorization and authentication

The following sections of the *Oracle Fusion Middleware Application Security Guide* provide details about implementing post-development authorization:

- Configuring Single Sign-On in the *Oracle Fusion Middleware Application Security Guide*.
- Mapping of Logical Roles to WebLogic Roles in the *Oracle Fusion Middleware Application Security Guide*.
- Migrating Application Policies with Fusion Middleware Control in the *Oracle Fusion Middleware Application Security Guide*.
- Managing the Domain Policy Store in the *Oracle Fusion Middleware Application Security Guide*.

2.3.3 Credential Store Framework

A credential store is a repository to store user name/password or generic credentials (a certificate). The value of using a credential store is that the application does not store passwords in clear text and does not have to invent its own solutions for protecting passwords, allowing administrators and developers alike to work with a consistent credential repository.

OPSS provides the Credential Store Framework for Create, Read, Update, and Delete operations on credentials stored in a credential store.

OPSS supports three types of credential stores:

- file-based
- LDAP directory
- Oracle Database

Domain-level identity and credential stores are supported for applications. You can configure credentials for automatic migration to the domain credential store when the application is deployed.

2.3.4 User and Role API

The User and Role API framework allows applications to access identity information (users and groups) in a uniform and portable manner regardless of the particular underlying identity repository. Supported operations include creating, updating, or deleting identities, or searching identities for attributes or information of interest. Through the identity store service, the framework also enables you to search multiple LDAP identity stores in a single query.

The repository could be an LDAP directory server such as Oracle Internet Directory, Oracle Directory Server Enterprise Edition, or Microsoft Active Directory, or could be a database, flat file, or some other custom repository.

The User and Role API framework provides a convenient way to access repositories programmatically in a portable way, freeing the application developer from the potentially difficult task of accounting for the intricacies of particular identity sources. The framework allows an application to work against different repositories seamlessly. An application can switch between various identity repositories without any code changes being required.

For details, refer to:

- Managing the Identity Store in the *Oracle Fusion Middleware Application Security Guide*
- Developing with the User and Role API in the *Oracle Fusion Middleware Application Security Guide*

2.3.5 Policy Store and the Policy API

The policy store holds the policies that are used to evaluate authorization decisions. It is a repository of system and application-specific policies and roles. Application roles can include:

- enterprise users and groups
- application roles, such as administrative roles

A policy can use any of these roles or users as principals.

The policy store can be shared by multiple applications in the same Oracle WebLogic Server domain and managed at the domain level.

In Oracle Fusion Middleware 11*g* Release 1 (11.1.1), policy stores can be:

- XML files, which are the out-of-the-box policy store provider
- LDAP directories

  - Oracle Internet Directory
  - Oracle Virtual Directory
- Oracle Database

The Policy Store API defines:

- A management interface to grant and revoke permissions to or from grantees
- A delegation architecture where authorization decisions can be delegated to custom policy providers based on configured criteria such as permission types and application names
- Application-based logical roles (or application roles) combined with application-specific fine-grained policies for portable representation of sophisticated application policies

For details, see "Understanding Identities, Policies, and Credentials" in the *Oracle Fusion Middleware Application Security Guide*.

2.3.6 Single Sign-On

Single sign-on enables a user to authenticate once and gain access to several applications without the need to re-authenticate.

Oracle WebLogic Server offers these single sign-on choices:

- Oracle Single Sign-On,
- Oracle Access Manager.

Oracle WebLogic Server includes two identity assertion providers (one for each solution) that can be configured with the Oracle WebLogic Administration Console. Applications running on Oracle WebLogic Server can choose either single sign-on solution (or both).

Additionally, Oracle Fusion Middleware provides a framework allowing any third-party single sign-on solution to be integrated with the environment.

For details about configuring your application to use single sign-on, see Configuring Single Sign-On in the *Oracle Fusion Middleware Application Security Guide*.

2.3.7 SSL Support

Oracle Fusion Middleware offers SSL configuration features to provide SSL configuration across the enterprise stack:

- Web Tier
  - Oracle HTTP Server
  - Oracle Web Cache
- Middle Tier
  - Oracle SOA Suite

    Oracle WebCenter

    Oracle Identity Federation
- Data Tier
  - Oracle Internet Directory
  - Oracle Virtual Directory

  - Oracle Database
  - third-party LDAP directories and databases
- Oracle WebLogic Server, including SSL inbound from Oracle HTTP Server to Oracle WebLogic Server

The Oracle Enterprise Manager Fusion Middleware Control GUI tool and the `WLST` command-line tool provide consistent, uniform functions for configuring Oracle wallets and JKS keystores, and configuring SSL. These tools also provide the key functionality of existing tools such as `orapki`.

Appropriate tools, such as the Oracle WebLogic Server Administration Console, are available for SSL-enabling other endpoints.

For details, see these chapters in the *Oracle Fusion Middleware Administrator's Guide*:

- Managing Keystores, Wallets, and Certificates
- SSL Configuration in Oracle Fusion Middleware
- Oracle Wallet Manager and orapki

2.3.8 Auditing

The Common Audit Framework service in Oracle Fusion Middleware 11*g* Release 1 (11.1.1) provides a central audit facility for the middleware family of products. The audit service:

- is usable across Oracle Fusion Middleware 11*g* components and services such as Oracle Web Services Manager, Oracle Internet Directory (OID), Oracle Virtual Directory, and Oracle Directory Integration and Provisioning (DIP)
- is available to Java SE applications that run outside the application server container
- integrates with Oracle Enterprise Manager Fusion Middleware Control for UI-based configuration and management
- integrates with `WLST` for command-line, script-based configuration
- integrates with Oracle Platform Security Services

Key features of auditing for robust support of compliance and analytics needs include:

- A uniform system for administering audits across a range of system components, Java EE and non-JavaEE applications
- Capturing authentication history/failures, authorization history, user management, and other common transaction data
- Analytics on fraud and intrusion detection
- Flexible audit policies, including pre-seeded audit policies, capturing customers' most common audit events
- Prebuilt compliance reporting features using out-of-the-box analytical reporting capabilities within Oracle BI Publisher; data can be analyzed on multiple dimensions across multiple components. These reports can also be customized according to your preferences.
- Common audit repository
- Common audit record format

See the following topics in the *Oracle Fusion Middleware Application Security Guide* for more information:

- Introduction to Common Audit Framework
- Configuring and Managing Auditing

2.3.9 Oracle Security Developer Toolkit

Oracle Security Developer Tools provide you with the cryptographic building blocks necessary for developing robust security applications, ranging from basic tasks like secure messaging to more complex projects such as securely implementing a service-oriented architecture. The tools build upon the core foundations of cryptography, public key infrastructure, web services security, and federated identity management, and are widely used in building Oracle's own security offerings.

Oracle Products using Oracle Security Developer Tools

Products using the toolkit include, but are not limited to:

- Oracle Applications
  - Global Mapping; GI (Image Process Management); Payment; XDO (XML Publisher); Workflow, BPEL
  - Oracle Collaboration Suite (Email)
- Application Server
  - Available on WebLogic Server (10.3 and later)
- Platform Security
  - Oracle Platform Security Services
  - SSL Configuration
  - Oracle Wallet (used by Oracle Identity Management products, Fusion Middleware Control and the Oracle Database Server)
- Oracle Products
  - Oracle Web Services Manager (OWSM)
  - Business Integration (B2B)
  - Oracle Portal
  - Oracle Identity Federation (OIF)

What's in the Oracle Security Developer Tools

The toolkit includes:

- Oracle Crypto - supports Public key cryptography algorithms, Digital signature algorithms, Key exchange algorithms, Symmetric cryptography algorithms, Message digest algorithms, MAC algorithms, and methods for building and parsing ASN.1 objects
- Oracle Security Engine - The Oracle Security Engine toolkit supports X.509 Version 3 Certificates, PKCS#12, PKCS#10 for certificate requests, CRLs, Signed Public Key And Challenge (SPKAC), PKCS#7 for wrapping X.509 certificates and CRLs, and other features.
- Oracle CMS - provides an extensive set of tools for reading and writing CMS objects, and supporting tools for developing secure message envelopes.

- Oracle S/MIME - provides full support for X.509 Version 3 certificates with extensions, including certificate parsing and verification; support for X.509 certificate chains in PKCS#7 and PKCS#12 formats; private key encryption using PKCS#5, PKCS#8, and PKCS#12; and an integrated ASN.1 library for input and output of data in ASN.1 DER/BER format.
- Oracle PKI - contains a set of tools for working with digital certificates, including access to LDAP directories, date stamping of digital messages, certificate validation, and certificate management.
- Oracle JCE - is a cryptographic provider that fits into the Sun Microsystems JCA provider framework. Oracle JCE implements the standard JCE APIs. The Oracle JCE Provider package contains several cryptographic algorithms and services including ciphers, key agreement, key factory and secret key factory, key pair generation, and others.

  The standard API enables the developer to conveniently switch from one provider to another.
- Oracle XML Security - supports the XML Digital Signature specification (JSR105), the Decryption Transform proposed standard, the XML Canonicalization standard, the Exclusive XML Canonicalization standard, and compatibility with a wide range of JAXP 1.1 compliant XML parsers and XSLT engines.
- Oracle SAML - provides tools and documentation to assist developers of SAML-compliant Java security services. You can integrate Oracle SAML into existing Java solutions, including applets, applications, EJBs, servlets, and JSPs. The API supports:
  - the SAML 1.0/1.1 and 2.0 specifications
  - SAML-based single sign-on, Attribute, Metadata, Enhanced Client Proxy, and federated identity profiles
- Oracle Web Services Security - provides an authentication and authorization framework based on OASIS specifications, and supports the SOAP Message Security standard, the Username Token Profile standard, the X.509 Certificate Token Profile standard, and the WSS SAML Token Profile.
- Oracle Liberty - allows Java developers to design and develop single sign-on and federated identity solutions based on the Liberty Alliance specifications.
- Oracle XKMS - provides a convenient way to handle public key infrastructures by allowing developers to write XML transactions for digital signature processing. Oracle XKMS implements the W3C XKMS standard.

For details, see the *Oracle Fusion Middleware Reference for Oracle Security Developer Tools*.

3

Developing Secure Applications

This chapter provides an overview of Oracle Application Development Framework security and JavaEE security features.

3.1 ADF Security

This section contains these topics:

3.1.1 About Oracle ADF

The Oracle Application Development Framework (Oracle ADF) is an end-to-end application framework that builds on Java Platform, Enterprise Edition (Java EE) standards and open-source technologies to simplify and accelerate implementing service-oriented applications. For enterprise solutions that search, display, create, modify, and validate data using web, wireless, desktop, or web services interfaces, Oracle ADF can simplify the development effort.

Used in tandem, Oracle JDeveloper 11g and Oracle ADF give you an environment that covers the full development life cycle from design to deployment, with drag-and-drop data binding, visual UI design, and team development features built in.

Applications you build using the Fusion web technology stack achieve a clean separation of business logic, page navigation, and user interface by adhering to a model-view-controller architecture.

The core module in the framework is Oracle ADF Model, a declarative data binding facility that implements the JSR-227 specification. The Oracle ADF Model layer enables a unified approach to bind any user interface to any business service, without having to write code. The other modules that comprise a Fusion web application technology stack are:

- Oracle ADF Business Components, which simplifies building business services.
- Oracle ADF Faces rich client, which offers a rich library of AJAX-enabled UI components for web applications built with JavaServer Faces (JSF).

- Oracle ADF Controller, which integrates JSF with Oracle ADF Model. The ADF Controller extends the standard JSF controller by providing additional functionality, such as reusable task flows that pass control not only between JSF pages, but also between other activities, for instance method calls or other task flows.

3.1.2 About Oracle ADF Security

The Oracle ADF Security framework is the preferred technology to provide authentication and authorization services to the Fusion web application. A prime reason is that Oracle ADF Security is built on top of the Oracle Platform Security Services (OPSS) architecture, which provides a critical security framework and is itself well-integrated with Oracle WebLogic Server.

Note: Oracle ADF's built-in support for security features including OPSS features helps reduce the effort that would be required to implement those features outside Oracle ADF; indeed, certain features are not available using only container-managed security.

While other security-aware models exist that can handle user login and resource protection, Oracle ADF Security is ideally suited to provide declarative, permission-based protection for ADF bounded task flows, top-level web pages that use ADF bindings (pages that are not contained in a bounded task flow), and at the lowest level of granularity, rows of data defined by ADF entity objects and their attributes. In this document, these specific resources that the ADF Security framework protects are known as ADF security-aware resources.

You enable ADF Security for Fusion web applications when you run the Configure ADF Security wizard. The wizard configures ADF Security for the entire Fusion web application, so that any web page associated with an ADF security-aware resource is protected by default. Thus, after you enable ADF Security, your application is locked down so that the pages are considered secure by default.

After you enable ADF Security you must grant users access rights so that they may view the web pages of the Fusion web application. Access rights that you grant users are known as a security policy that you specify for the page's corresponding ADF security-aware resource. Ultimately, it is the security policy on the ADF resource that controls the user's ability to enter a task flow or view a web page.

Because ADF Security is based on Java Authentication and Authorization Service (JAAS), security policies identify the principal (the user or application role), the ADF resource, and the permission (an operation defined by the resource's ADF permission class). For example, the StoreFront module of the Fusion Order Demo application secures the web pages contained by the checkout-task-flow task flow to grant access only to logged-in users (also known as authenticated users).

At run-time, the Oracle ADF Security framework performs permission checking against the task flow's security policy to determine the user's right to complete the view operation. In this case, the security policy must grant the view permission to the user if they are to complete the checkout process.

The Containment Hierarchy

To simplify the task of defining security policies for users and ADF resources, ADF Security defines a containment hierarchy that lets you define one security policy for the ADF bounded task flow and its contains web pages. In other words, when you define the security policy at the level of the bounded task flow, you protect:

- the flow's entry point, and
- all pages within that flow

Role-Based Security

Instead of granting access to individual users, you group users into application roles and grant the view permission to the role. This simplifies configuration and improves the security administrator's ability to manage permissions.

For more information, see Understanding Users and Roles in the *Oracle Fusion Middleware Application Security Guide*.

Documented Procedures

Documented procedures in the *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework* explain these and other topics:

- How to Enable Oracle ADF Security using the Configure ADF Security wizard
- How to create application roles
- How to make an ADF resource public
- How to create test users and associate them with application roles
- How to create a login page and a welcome page
- How to Configure, Deploy, and Run a Secure Application in JDeveloper

3.1.3 Using Oracle ADF Security

This section provides an overview of how you use Oracle ADF Security.

Use the Security Wizard

To simplify the configuration process which enables Oracle ADF Security to integrate with OPSS, JDeveloper provides the Configure ADF Security wizard. The wizard is the starting point for securing the Fusion web application using Oracle ADF Security. The wizard is an application-level tool that, once run, enables ADF Security for all user interface projects that your application contains.

The Configure ADF Security wizard enables you to choose to enable authentication and authorization separately.

- Although ADF Security leverages Java EE container-managed security for authentication, enabling authentication lets you use the ADF authentication servlet to support user login and logout, but define container-managed security constraints to secure web pages.
- Enabling authorization means you intend to control access to the Fusion web application by creating security policies on ADF resources.

The wizard configures ADF Security for the entire Fusion web application, so that any web page associated with an ADF security-aware resource is protected; thus, your application is locked down so that the pages are considered secure by default.

Create Application Roles

Application roles represent the policy requirements of the application and define groups of users with the same access rights. The application roles that you create in the application policy store are specific to your application.

At run-time, access rights are conferred on the user through the application role of which the user is as a member. Thus, before you can define security policies (described below), the policy store must contain the application roles to which you intend to issue grants.

Grant the Security Policy

After you enable ADF Security you must grant users access rights so that they may view the web pages of the Fusion web application. Access rights that you grant users are known as a security policy that you specify for the page's corresponding ADF security-aware resource. Ultimately, it is the security policy on the ADF resource that controls the user's ability to enter a task flow or view a web page.

Create Test Users

JDeveloper provides editors to help you create both the identity and policy stores in an application-specific file repository. The list of valid user IDs and their assigned passwords is stored in the identity store section of the file.

The same editor lets you create application roles and assign the test users or enterprise roles as members of the application roles. (To enable the user to view resources, you make grants against application roles rather than against the users who are the members of those roles.)

Create a Login Page

Oracle ADF Security provides for implicit and explicit authentication:

- In an implicit authentication scenario, authentication is triggered dynamically if an unauthenticated user tries to access a web page associated with ADF security-aware resources not granted to the anonymous role. After login, another check verifies whether the authenticated user has view access granted on the requested page's ADF security-aware resource.
- In an explicit authentication scenario, your application has a public page that displays a login link, which, when clicked, triggers an authentication challenge to log in the user. The login link may optionally specify some other target page that should be displayed (assuming the authenticated user has access) after the successful authentication.

Test Security in JDeveloper

Oracle JDeveloper's Integrated WLS enables you to run the application directly within JDeveloper and determine whether to migrate security objects, including the application policies, users, and credentials that your application defines. By default, all security objects are migrated to Integrated WLS each time you run the application.

Documented Procedures

Documented procedures in the Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework describe these and other topics:

- Using the Security Wizard
- Creating Application Roles
- Defining ADF Security Policies
- Creating Test Users
- Creating a Login Page
- Testing Security in JDeveloper

3.2 JavaEE Security

Although you can leverage OPSS security capabilities through the OPSS APIs, there is no GUI support for configuration; you must hand-edit deployment descriptors to implement the features.

3.3 End-to-End Security Example

For an end-to-end example of implementing security in Oracle Fusion Middleware, from development to testing through deployment, refer to the Oracle Technology Network:

http://www.oracle.com/technology/products/id_mgmt/opss/index.html

4

Infrastructure Hardening

This chapter contains the following topics:

4.1 What is Infrastructure Hardening?

Infrastructure hardening is the act of applying security to each component of the infrastructure, including:

- Web servers,
- application servers,
- identity and access management solutions, and
- database systems.

> **Note:** Oracle WebLogic Server uses a more specific type of hardening known as lockdown, which refers to securing the subsystems and applications that run on a server instance. In contrast, infrastructure hardening is more general and involves doing a security survey to determine the threat model that may impact your site, and identifying all aspects of your environment (such as components in the Web tier) that could be insecure.

More specifically, Oracle Fusion Middleware administrators focus on these aspects of infrastructure security:

- SSL-enabling components and component routes, for example Oracle Web Cache to Oracle HTTP Server
- SSL-enabling web services
- managing ports and other features of the site such as:
  - default deployed application
  - demonstration,

  - and samples management
- Password management

4.2 Keystores

Objects necessary for SSL communication, including private keys, digital certificates, and trusted CA certificates are stored in keystores.

Oracle Fusion Middleware provides two types of keystores for keys and certificates:

- JKS-based keystore and truststore

  A JKS keystore is the default JDK implementation of Java keystores provided by Sun Microsystems. In 11gR1, all Java components and JavaEE applications use the JKS-based KeyStore and TrustStore.

  You use a JKS-based keystore for the following:

  - Oracle Virtual Directory
  - Applications deployed on Oracle WebLogic Server, including:
    * Oracle SOA Suite
    * Oracle WebCenter
- Oracle wallet

  An Oracle wallet is a keystore for credentials, such as certificates, certificate requests, and private keys.

  You use an Oracle Wallet for the following components:

  - Oracle HTTP Server
  - Oracle Web Cache
  - Oracle Internet Directory

For details, see " Managing Keystores, Wallets, and Certificates" in the *Oracle Fusion Middleware Administrator's Guide*.

4.3 Enabling SSL

SSL management capabilities in 11*g* Release 1 (11.1.1) are as follows:

- Oracle WebLogic Server provides SSL capability for client and server communications
- Oracle Fusion Middleware 11g offers an SSL configuration capability which supports SSL enablement for these Oracle Fusion Middleware system components:
  - Oracle Web Cache
  - Oracle HTTP Server
  - Oracle Internet Directory
  - Oracle Virtual Directory

The SSL configuration feature:

- abstracts the steps involved in configuring SSL from other management tasks

- makes SSL configuration consistent and uniform across all Oracle Fusion Middleware system components
- validates SSL during configuration
- provides default values for various SSL parameters to simplify configuration
- includes the Oracle SSL Automation Tool, which enables you to configure multiple components in a domain using a domain-specific CA certificate.

SSL Configuration Tools in Oracle Fusion Middleware

Depending on the task, a range of configuration tools are available:

- Oracle Enterprise Manager Fusion Middleware Control and the `WLST` command-line tool to SSL-enable listeners for system components and to manage Oracle wallets and JKS keystores for those components
- Oracle Wallet Manager and the `orapki` command-line tool for Oracle wallets

Refer to the following for details:

- SSL Configuration in Oracle Fusion Middleware in the *Oracle Fusion Middleware Administrator's Guide*
- Managing Keystores, Wallets, and Certificates in the *Oracle Fusion Middleware Administrator's Guide*

SSL Configuration Tools in Oracle WebLogic Server

Oracle Weblogic Server uses these tools to manage keystores and enable SSL on connections coming into the server:

- the JDK `keytool` utility

  Oracle WebLogic Server supports the Java KeyStore (JKS) provided by the JDK. The `keytool` utility is used to manage keystores in addition to creating key pairs, and generating and reading self-signed certificates.

- The WebLogic Server administrator console

  This console is used to manage the SSL configuration of WebLogic Server listeners. For example, Oracle SOA Suite and Oracle WebCenter running on Oracle WebLogic Server use these facilities to enable SSL.

Refer to the following documents for details:

- Getting Started with Oracle WebLogic Server Administration Console in the *Oracle Fusion Middleware Administrator's Guide*
- The *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*

4.4 Port and Environment Management

Documented procedures for ports management address the following topics:

- In a firewall protected deployment environment, how do we keep the number of ports open to a minimum
- How to manage and administer the ports in such an environment

Oracle also recommends the following best practices for handling default, demonstrations and samples that are shipped with the product:

- Remove unneeded default applications

- Restrict access to administrative applications
- Restrict access to deployed applications

For more information, see Managing Ports in the *Oracle Fusion Middleware Administrator's Guide*.

4.5 Password Management

In Oracle Fusion Middleware 11gR1, Oracle recommends storing passwords in the Credential Store rather than in `connection.xml` or `data-sources.xml` files.

The Credential Store Framework in Oracle Platform Security Services provides a mechanism for securely storing and managing credentials for any Java-based (Java SE and Java EE) applications. It is designed to hold account information, user names and passwords for connecting to any systems that applications must access.

4.6 Lockdown

The WebLogic Security Service provides a powerful and flexible set of software tools for securing the subsystems and applications that run on a server instance. For details, see "Securing Applications" in the document titled *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*.

5 Common Security Scenarios and Tasks

This chapter lists the most common security scenarios and tasks of interest to security administrators and developers. Links provide drill-down details on the concepts and how to implement security features in Oracle Fusion Middleware.

Topics include:

- Single Sign-On
- Summary of Common Security Tasks
- Task-Based References

5.1 Single Sign-On

This section explains the products and deployment options for single sign-on in 11*g* Release 1 (11.1.1). Topics include:

- Single Sign-On Options
- Deployment Scenarios

5.1.1 Single Sign-On Options

Oracle Fusion Middleware supports many single sign-on options in 11*g* Release 1 (11.1.1). Oracle WebLogic Server provides single sign-on support through Security Assertion Markup Language (SAML) and Windows Native Authentication. In addition, identity assertion providers are also available for Oracle WebLogic Server to integrate with Oracle Access Manager which is the recommended enterprise-grade single sign-on solution from Oracle Identity Management. This offers a variety of choices for customers to choose from, depending on their needs.

See Also:

- Section 1.2.1, "About Authentication and Single Sign-On"
- Configuring Single Sign-On in Oracle Fusion Middleware in the *Oracle Fusion Middleware Application Security Guide*

5.1.2 Deployment Scenarios

This section describes some common single sign-on scenarios in 11*g* Release 1 (11.1.1):

- Setting up Oracle SOA or Oracle WebCenter 11g for the First Time
- Setting up Oracle SOA or Oracle WebCenter 11g with existing Oracle Application Server

- Setting up 11g Portal, Forms, Reports or Discover
- Setting up Oracle SOA or Oracle WebCenter 11g with 11g Portal, Forms, Reports or Discover
- Setting up 11g Oracle Fusion Middleware with Oracle E-Business Suite
- Delegating Authentication from Oracle Single Sign-On to Oracle Access Manager

5.1.2.1 Setting up Oracle SOA or Oracle WebCenter 11g for the First Time

This scenario involves setting up Oracle SOA or Oracle WebCenter 11*g* Release 1 (11.1.1) for the first time with no previous Release 10*g* Application Server deployments.

In this scenario the customer has no previous Oracle Application Server deployment. The recommended single sign-on solution is Oracle Access Manager which allows customer to use Oracle Internet Directory or other LDAP servers of choice as the user and group repository.

5.1.2.2 Setting up Oracle SOA or Oracle WebCenter 11g with existing Oracle Application Server

This scenario involves setting up Oracle SOA or Oracle WebCenter 11*g* Release 1 (11.1.1) with existing Oracle Application Server Release 10*g* deployment where Oracle Internet Directory and Oracle Single Sign-On are used.

The customer is currently using Oracle Internet Directory as the user and group repository and Oracle Single Sign-On as the single sign-on solution in the 10*g* deployment. The 11*g* Release 1 (11.1.1) Oracle SOA or Oracle WebCenter deployment continues to rely on this Oracle Internet Directory and Oracle Single Sign-On infrastructure for single sign-on and user repository.

5.1.2.3 Setting up 11g Portal, Forms, Reports or Discover

Whether or not the customer has an existing 10*g* Oracle Application Server deployment, the 11*g* Release 1 (11.1.1) Portal, Forms, Reports and Discover only work with Oracle Internet Directory and Oracle Single Sign-On.

5.1.2.4 Setting up Oracle SOA or Oracle WebCenter 11g with 11g Portal, Forms, Reports or Discover

Because of the requirement in Section 5.1.2.3, "Setting up 11g Portal, Forms, Reports or Discover", this scenario also defaults to having Oracle Internet Directory and Oracle Single Sign-On as the recommended solution.

5.1.2.5 Setting up 11g Oracle Fusion Middleware with Oracle E-Business Suite

Oracle E-Business Suite 11/12 can integrate with Oracle Internet Directory and Oracle Single Sign-On. Where Oracle Internet Directory and Oracle Single Sign-On are used as an enterprise solution, they can continue to be used with 11*g* Release 1 (11.1.1) Oracle Fusion Middleware.

5.1.2.6 Delegating Authentication from Oracle Single Sign-On to Oracle Access Manager

While many of the scenarios mandate Oracle Single Sign-On to be the single sign-on solution, it is possible to delegate the authentication to an Oracle Access Manager instance. The scenario positions Oracle Access Manager as the enterprise solution while supporting components that only integrate with Oracle Single Sign-On - by

having Oracle Single Sign-On delegating all authentication requests to Oracle Access Manager. This is also known as the "bridge" solution and is applicable to all scenarios where Oracle Single Sign-On is mandatory. Please note that Oracle Internet Directory is required to be the user and group repository in all cases.

5.2 Summary of Common Security Tasks

Table 5–1 lists the most common security tasks for the Oracle Fusion Middleware administrator, and the tool(s) used for each task.

Table 5–1 Common Security Tasks

Frequency	Task Description	Tools	Notes
One-time	SSL enable Oracle HTTP Server, Oracle WebCache, Oracle Internet Directory, Oracle Virtual Directory and Oracle WebLogic Server	Fusion Middleware Control for: ■ Oracle HTTP Server ■ Oracle WebCache ■ Oracle Internet Directory ■ Oracle Virtual Directory Keytool and WebLogic Server Administration Console for Oracle WebLogic Server	
	Change Policy Store and Credential Store to Oracle Internet Directory	Fusion Middleware Control, and Oracle Internet Directory commands	
	Configure Oracle Access Manager as Single Sign-On for Oracle Fusion Middleware	Fusion Middleware Control	
	Configure Authenticators	WebLogic Server Administration Console	
	Set up keystore for Oracle Web Services Manager	Java keytool utility	
	Configure OPSS login modules (like Kerberos) for Oracle Web Services Manager	Fusion Middleware Control	
Frequent	Configure application security when deploying applications	When deploying Oracle ADF or OPSS-based applications, use Fusion Middleware Control When deploying JavaEE applications, use WebLogic Server Administration Console	

Table 5–1 (Cont.) Common Security Tasks

Frequency	Task Description	Tools	Notes
	Manage application role-to-enterprise group mapping after deploying application	Fusion Middleware Control or WLST	Applicable to Oracle ADF or OPSS-based applications. Can be scripted using WLST for frequent operations.
	Manage credentials used by the application	Fusion Middleware Control or `WLST`	Applicable to Oracle ADF or OPSS-based applications. Can be scripted using `WLST` for frequent operations.
	Configure Oracle Web Services Manager policies for web services and clients	Fusion Middleware Control	
	Configure Oracle Web Services Manager client user credentials in OPSS Credential store	Fusion Middleware Control or `WLST`	
	Attach/Detach Oracle Web Services Manager policies to web services and clients		
	Configure Audit Store		
	Configure Audit Policies	Fusion Middleware Control or `WLST` for most components	
	View audit reports for Fusion Middleware components	Oracle Business Intelligence Publisher	

5.3 Task-Based References

This section provides links to Oracle Fusion Middleware security documentation, including conceptual, administration, and development topics. Based on a develop-deploy-administer flow, it is organized in these sub-sections:

- References for Security Tasks During Development
- References for Security Tasks During Deployment
- References for Authentication
- References for Authorization
- References for SSL
- References for Auditing
- References for Logging and Diagnostics

5.3.1 References for Security Tasks During Development

Developing with Oracle ADF

In the Oracle Fusion Middleware Documentation Library, see these items under Popular Tasks:

- ADF Tasks
- Security Tasks

Developing with Oracle Platform Security Services

- Developing Authentication in the *Oracle Fusion Middleware Application Security Guide*
- Developing Authorization in the *Oracle Fusion Middleware Application Security Guide*
- Developing with the User and Role API in the *Oracle Fusion Middleware Application Security Guide*

Portlet Security

Securing Your WebCenter Application in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*

Programming Oracle WebLogic Server Security

- Securing Web Applications in the *Oracle Fusion Middleware Programming Security for Oracle WebLogic Server*
- Securing Enterprise JavaBeans (EJBs) in *Oracle Fusion Middleware Programming Security for Oracle WebLogic Server*

Developing Security Providers for Oracle WebLogic Server

- Introduction to Developing Security Providers for WebLogic Server in the *Oracle Fusion Middleware Developing Security Providers for Oracle WebLogic Server*
- Authentication Providers in the *Oracle Fusion Middleware Developing Security Providers for Oracle WebLogic Server*
- Authorization Providers in the *Oracle Fusion Middleware Developing Security Providers for Oracle WebLogic Server*

Developing applications for Oracle Internet Directory, Oracle Directory Integration Platform, and Oracle Single Sign-On

Developing Applications for Oracle Identity Management in the *Oracle Fusion Middleware Application Developer's Guide for Oracle Identity Management*

5.3.2 References for Security Tasks During Deployment

Deploying JavaEE Applications

- Deploying, Undeploying and Redeploying JavaEE Applications in the *Oracle Fusion Middleware Administrator's Guide*
- Using Platform Security Services to Secure JavaEE applications
  - Manually Configuring JavaEE Applications to Use OPSS in the *Oracle Fusion Middleware Application Security Guide*

  - Security Administration in the *Oracle Fusion Middleware Application Security Guide*

- Using JavaEE Security to Secure JavaEE Applications
  - Managing Security for Web Applications and EJBs in the Oracle WebLogic Server Administration Console Online Help
  - Using Declarative Security With Web Applications in *Oracle Fusion Middleware Programming Security for Oracle WebLogic Server*
  - Using Declarative Security With EJBs in *Oracle Fusion Middleware Programming Security for Oracle WebLogic Server*

Deploying Oracle Application Development Framework Applications

- Deploying Secure Applications in the *Oracle Fusion Middleware Application Security Guide*
- Managing Application Roles in the *Oracle Fusion Middleware Application Security Guide*
- Managing Application Policies in the *Oracle Fusion Middleware Application Security Guide*

Securing Oracle WebLogic Server Web Services

- When Should You Use Oracle WS-Security Policies? in *Oracle Fusion Middleware Securing WebLogic Web Services for Oracle WebLogic Server*
- Configuring Message-Level Security in *Oracle Fusion Middleware Securing WebLogic Web Services for Oracle WebLogic Server*
- Configuring Transport-Level Security in *Oracle Fusion Middleware Securing WebLogic Web Services for Oracle WebLogic Server*

Securing SOA Web Services

- Understanding Oracle WSM Policy Framework in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*
- Managing Web Services policies in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*
- Attaching Policies to Web Services in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*
- Configuring Policies in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*

Directory Administration

- Getting Started With Oracle Internet Directory in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- Getting Started with Administering Oracle Virtual Directory in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*

Directory Integration and Provisioning

- Synchronization Using Oracle Directory Integration Platform in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*
- Provisioning with the Oracle Directory Integration Platform in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*

- Integrating with Third-Party Directories in the *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*

High Availability

Configuring High Availability for Identity Management Components in the *Oracle Fusion Middleware High Availability Guide*

5.3.3 References for Authentication

Java Applications

- Oracle Single Sign-on - Configuring Oracle Single Sign-On in the *Oracle Fusion Middleware Application Security Guide*
- Oracle Access Manager - Configuring Oracle Single Sign-On in the *Oracle Fusion Middleware Application Security Guide*

Oracle Identity Federation

- Deploying Oracle Identity Federation in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
- Configuring Oracle Identity Federation in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
- Server Administration in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*

5.3.4 References for Authorization

Coarse-Grained Authorization

OPSS Authorization and the Policy Store in the *Oracle Fusion Middleware Application Security Guide*

Fine-Grained Authorization

Creating an Entitlement Set in the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*

Creating an Application Role in the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*

Managing Delegated Applications in the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*

Delegating With Administrator Roles in the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*

Managing Application Resource Types in the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*

Finding Objects with a Simple Search in the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*

Mapping an External User to an Application Role in the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*

Mapping External Roles to an Application Role in the *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server*

5.3.5 References for SSL

SSL communication is available for Oracle Fusion Middleware components and applications in each tier:

- SSL for the Web Tier
  - Enabling SSL for Oracle Web Cache Endpoints in the *Oracle Fusion Middleware Administrator's Guide*
  - Enabling SSL for Oracle HTTP Server Virtual Hosts in the *Oracle Fusion Middleware Administrator's Guide*
- SSL for the Middle Tier
  - Configure SSL for Oracle WebLogic Server in the *Oracle Fusion Middleware Administrator's Guide*
  - Configure SSL for Oracle SOA Suite in the *Oracle Fusion Middleware Administrator's Guide*
  - Configure SSL for Oracle WebCenter in the *Oracle Fusion Middleware Administrator's Guide*
  - Configuring SSL for Oracle Identity and Access Management in the *Oracle Fusion Middleware Administrator's Guide*
  - SSL-enable Oracle Reports, Forms, Discoverer, and Portal in the *Oracle Fusion Middleware Administrator's Guide*
  - Client-side SSL for Applications in the *Oracle Fusion Middleware Administrator's Guide*
- SSL for the Data Tier
  - Enabling SSL on Oracle Internet Directory Listeners in the *Oracle Fusion Middleware Administrator's Guide*
  - Enabling SSL on Oracle Virtual Directory Listeners in the *Oracle Fusion Middleware Administrator's Guide*
  - Configure SSL for the Database in the *Oracle Fusion Middleware Administrator's Guide*

5.3.6 References for Auditing

Concepts and Administration

- Introduction to Oracle Fusion Middleware Audit Framework in the *Oracle Fusion Middleware Application Security Guide*
- Configuring and Managing Auditing in the *Oracle Fusion Middleware Application Security Guide*

Audit Reporting

For enterprise deployments, especially those taking advantage of the extensive auditing capabilities of Oracle Identity Management, it is highly recommended that you deploy a dedicated enterprise-class reporting solution. Oracle Business Intelligence Publisher provides such a solution with the flexibility, automation, and performance required for large-scale operations.

Several Oracle Identity Management components provide reports to enable you to keep track of audited events. See the following documents for details:

- About Audit Reports and Oracle Business Intelligence Publisher in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.
- Oracle Adaptive Access Manager Reports Reference in the *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.
- Using Reporting Features in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.
- Using Audit Analysis and Reporting in the *Oracle Fusion Middleware Application Security Guide*.

> **See Also:** *Oracle Business Intelligence Publisher Administrator's and Developer's Guide* for details about about using and managing Oracle Business Intelligence Publisher.

5.3.7 References for Logging and Diagnostics

- Managing Log Files and Diagnostic Data in the *Oracle Fusion Middleware Administrator's Guide*
- Diagnosing Problems with Oracle WSM Policy Manager in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*

Index

P

R

S

T

U

W

X