Oracle® Fusion Applications Security Hardening Guide

11*g* Release 6 (11.1.6)

Part Number E16690-06

September 2012

Oracle® Fusion Applications Security Hardening Guide

Part Number E16690-06

Author: Tina Brand

Contributor: Uppili Srinivasan

Contents

Preface

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

Oracle Fusion Applications Help

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

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

Oracle Fusion Applications Guides

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

Note
The **Guides** menu also provides access to the business process models on which Oracle Fusion Applications is based.

Guides are designed for specific audiences:

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

- **Security Reference Manuals** describe the predefined data that is included in the security reference implementation for one offering. They are intended for implementors, security administrators, and auditors. They are organized by role.

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

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

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

Other Information Sources

My Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

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

Oracle Enterprise Repository for Oracle Fusion Applications

Oracle Enterprise Repository for Oracle Fusion Applications provides visibility into service-oriented architecture assets to help you manage the lifecycle of your software from planning through implementation, testing, production,

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

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

Documentation Accessibility

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

Comments and Suggestions

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

1

Security Hardening Methodology

Oracle Fusion Applications and Enterprise Deployment Guidance: Explained

Oracle Fusion Applications are secure as built by Oracle for general case installations. Business flows, including those for security administration, are secured using standard principles and best practices.

The Oracle Fusion Applications Enterprise Deployment Guide describes deployments that are secure out of the box and highly available.

Oracle Fusion Applications enterprise deployment guidelines are as widely applicable as possible for configurations based on a recommended architecture that is independent of hardware and operating systems. The deployment architecture leverages grid infrastructure and optimizes cost, performance, scale, and controls over recovery from interruptions or acceptable data loss from natural disaster.

Enterprise deployment guidance provides sufficient and optimum levels of security balanced for the performance requirements of a majority of common enterprises. Oracle Fusion Applications security architecture is built on a highly flexible Fusion Middleware security platform that allows further fine tuning to factor any special needs and requirements beyond those represented by the enterprise deployment guidelines.

Security hardening fits into the Oracle Fusion Applications deployment process as follows.

- Fusion Applications installation - laying down the bits
- Provisioning the basic topology
- Enterprise deployment for security and high availability following the enterprise deployment guidance
- Security hardening and fine tuning based on the assessment of the deployment environment relative to EDG recommendations.
- Functional setup

As deployments change, enterprises may choose to iterate their hardening and security fine tuning.

For details about application provisioning, see the Oracle Fusion Applications Installation Guide.

For details about enterprise deployment, see the Oracle Fusion Applications Enterprise Deployment Guide.

Oracle Fusion Applications Security Hardening: Explained

Hardening Oracle Fusion Applications focuses on points of exposure to security risks on the boundaries and end points of a deployment. Security professionals such as Oracle Fusion Applications implementation consultants, security administrators, IT security managers, and IT auditors are involved in hardening Oracle Fusion Applications. Oracle Fusion Applications presumes that security hardening decisions are based on analysis of risks and threats.

The methodology for analyzing specific deployment requirements and guidelines to fulfill those requirements augments hardening practices that may be documented separately for Oracle Fusion Middleware and Oracle Database components included in an Oracle Fusion Applications deployment.

Note

The methodology and guidelines assume an Oracle Fusion Applications installation with all product families and products licensed.

For information on the Oracle Fusion Applications security approach and implementation, see the Oracle Fusion Applications Security Guide.

Oracle Fusion Applications provides the provisioning tools and an Enterprise Deployment Guide (EDG) necessary for provisioning in an enterprise deployment topology that is end-to-end secured and optimized out of the box for the most common business cases.

Oracle Fusion Applications allows fine tuning to address requirements beyond the enterprise deployment guidance.

Important

For end-to-end security, EDG also assumes that the stipulated environmental requirements are fully implemented.

Requirements for additional security hardening and fine-tuning commonly result from differences in deployment environments compared to the conditions stipulated by the enterprise deployment guidance on the following.

- The network environment
- The trust model underlying personnel with administrative access
- Accommodation of user communities of interest (COI) with different levels of trust

- The audit and compliance requirements specific to an industry

A security hardening methodology involves assessing the circumstances where hardening may be required. Assessment consists of tailoring the security configuration of the Oracle Fusion Applications deployment blueprint to match the unique deployment environment and usage characteristics of a particular enterprise.

Network Environment Considerations

In an Oracle Fusion Applications deployment based on the enterprise deployment guidelines, by default all outward facing connections are SSL enabled and connections within the Oracle Fusion Applications infrastructure's protection zones are not SSL enabled. Additional SSL configuration and administration may become critical where SSL is not enabled, even where backchannel communications occur behind a demilitarized zone (DMZ). Oracle provides SSL configuration procedures specifically for Oracle Fusion Applications to simplify this process.

Administrative Trust Model Considerations

A particular business solution may include areas of risk that are orthogonal to the Fusion Applications deployment blueprint, such as the type of user communities, the network environments from which users need access to the services, or integration with third party products.

Industry Specific Audit and Compliance Requirements

Department of defense (DOD), government, and health care industry requirements increasingly emphasize not only the business process, but also the security of the deployment itself.

Security Hardening Information: Highlights

Information about security hardening of components in an Oracle Fusion Applications deployment is available in various documents.

Oracle Fusion Applications

Information on the applications tier in support of hardening Oracle Fusion Applications is available in various documents.

- For information on installing, provisioning, and deployment, refer to the following guides.

  See: Oracle Fusion Applications Installation Guide

  See: Oracle Fusion Applications Enterprise Deployment Guide

- For information on possible security administration tasks independent of enterprise deployment and hardening guidelines, refer to the Oracle Fusion Applications Administrator's Guide.

  See: Securing Oracle Fusion Applications

- For information on the security approach in Oracle Fusion Applications, refer to the Oracle Fusion Applications Security Guide.

  See: Security: Overview

Oracle Fusion Middleware

Information that is not specific to Oracle Fusion Applications deployments about hardening components in the middle tier is available in various documents.

- For information on securing your environment, refer to the Oracle Fusion Middleware Security and Administrator's Guide for Web Services.

  See: Setting Up Your Environment for Policies

  See: Defining a Trusted Distinguished Names List for SAML Signing Certificates

  - For additional information on multi-domain keystore hardening, refer to the Oracle Fusion Middleware Security and Administration Guide for Web Services.

    See: Multi-Domain Use Case

- For information on securing search, refer to the Oracle Secure Enterprise Search Administrator's Guide.

  See: Secure Search in Oracle Fusion Applications

Oracle Database

Information about Oracle Database hardening that is not specific to Oracle Fusion Applications is available in various documents.

- For information on database features certified for use with Oracle Fusion Applications, refer to the Oracle Database Advanced Security Administrator's Guide.

  See: Data Encryption and Integrity

- For information on configuring groups of database schemas and roles that must be secured to protect application data from database administrators (DBA) and other privileged users, refer to the Oracle Database Vault Administrator's Guide

  See: Configuring Realms

- For information on adding source databases to Oracle Audit Vault and then deploying collectors, refer to the Oracle Audit Vault Administrator's Guide.

  See: Registering Source Databases and Collectors

2

Hardening Backchannel Network and Services

Network Security: Overview

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

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

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

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

Note

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

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

For more information about default network security, see the Oracle Fusion Applications Enterprise Deployment Guide.

Network Security in Oracle Fusion Applications Enterprise Deployments: Explained

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

The following methods are most common in achieving network security.

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

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

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

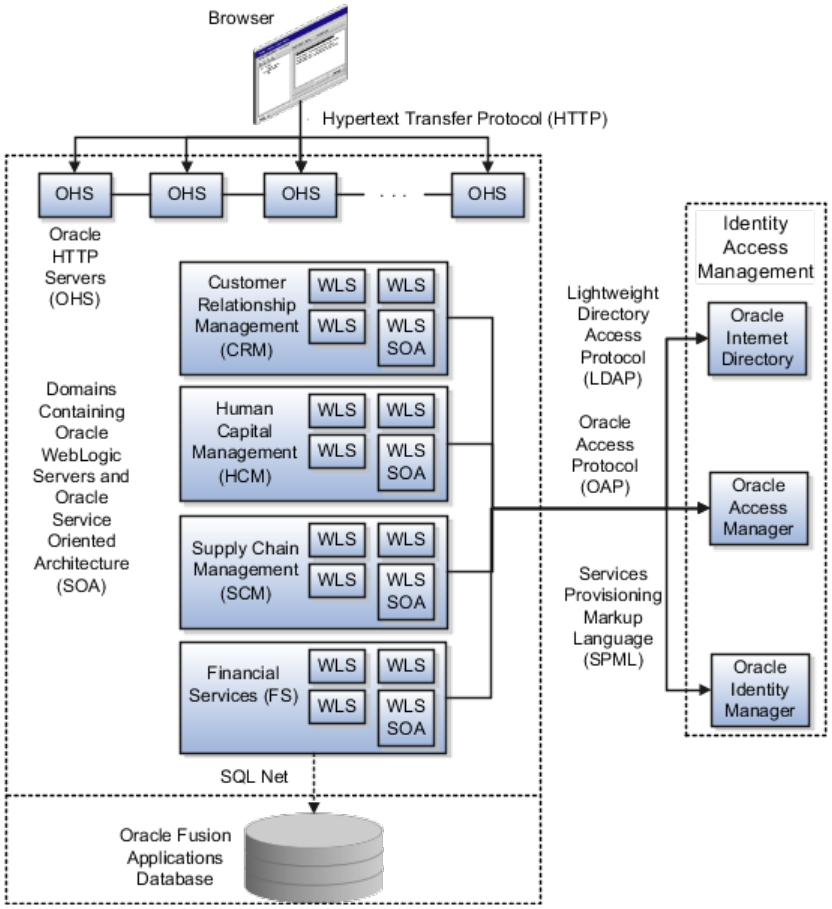
The network architecture of the enterprise deployment guidelines includes the following.

- The Web servers (Oracle HTTP Server (OHS)), the application servers (WebLogic Server (WLS)), and all other servers for your Oracle Fusion Applications instance run within a single isolated network.
- The Oracle Fusion Applications Database, Business Intelligence, Content Management, and Search services all run in either the same isolated network or each in its own isolated network that can only be reached via the applications private network.
- Centralized services such as Oracle Identity Management (OIM) servers are assumed to operate outside of these isolated networks.
- The connection to the database is assumed to be between two isolated networks.
- There are no connections to external Web services configured by initial provisioning.

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

The figure shows the connections that are SSL enabled in an Oracle Fusion Applications deployment. The connections among the Oracle WebLogic Servers (WLS) and domains of the Oracle Fusion Applications deployment are not SSL enabled because the enterprise deployment guidelines require and assume that

the subnets in the data center where Oracle Fusion Application is deployed are secured by network firewalls preventing direct access of Oracle Fusion Application components by users and applications outside the data center. The connection to the Oracle Fusion Applications database in an adjoining protected zone is also not SSL enabled. But connections to the identity access management components are SSL enabled.



For more information on configuring SSL in the generic case, see the Oracle Fusion Applications Administrator's Guide.

Network Security on Transactional Database Access: Critical Choices

Network Data Encryption and Data Integrity features of Oracle Advanced Security protect sensitive data when it is transmitted over the network by encrypting all communication between the client, the application server, and the database. This encrypts transactions end to end.

Data transmits in packets. Secure Socket Layers (SSL) and other network protections secure data in transit. Digital certificates encrypt or provide a hash digest of the data prior to transmission.

Network Database Encryption and Data Integrity

Oracle Database Advanced Security provides encryption algorithms to protect the privacy of network data transmissions such as the following.

- RC4 Encryption
- DES Encryption
- Triple-DES Encryption
- Advanced Encryption Standard

Based on the level of security and performance required for different types of data transfers, select a network encryption algorithm during configuration of Oracle Database Advanced Security.

Network encryption protects all data on the network, not selectively only some data.

Data integrity algorithms protect against attacks such as data modification, deleted packets and replay attacks. To ensure the integrity of data packets during transmission, use the Oracle Advanced Database Security cryptographically secure message digest (MD5 or SHA-1 hashing algorithms), which includes the digest with each message sent across a network.

For more information about network data encryption and integrity for oracle servers and clients, see the Oracle Database Advanced Security Administrator's Guide.

Sensitive Data In Transit

Your enterprise activates a configuration of encryption algorithms and negotiations depending on levels of security and performance for different types of data transfers. Network Data Encryption encrypts all data rather than selectively encrypting only some data.

Oracle Fusion Applications deploys with the following settings for client and server in Oracle Net Manager.

Encryption Type: `REQUIRED`

Checksum Level: `REQUIRED`

Oracle Advanced Security generates a cryptographically secure message digest using hashing algorithms and includes the digest with each message sent across a network to ensure the integrity of the data packets. These data integrity protections prevent data modification, deletion of replay attacks during transmission.

Non-SSL Encryption

Enable non-SSL encryption of SQL* Net network traffic by adding the following line to the listener.ora config file on the database server(s) and then bouncing the database TNS Listener.

```
SQLNET.ENCRYPTION_SERVER = REQUIRED
```

Additionally, to avoid weak protocols and add more seed, include the following lines.

```
SQLNET.ENCRYPTION_TYPES_SERVER= (AES256, AES192, 3DES168)
SQLNET.CRYPTO_SEED =
 <randomstring_for_this_deployment_up_to_70_characters>
```

For more information about configuring SSL for the database, see the Oracle Fusion Applications Administrator's Guide.

Network Security on Oracle Fusion Applications Search: Points to Consider

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

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

Hardening Oracle Fusion Applications Search

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

Settings for Oracle Fusion Applications Search with SSL Enabled on Windows

Ensure that the crawler script file %ORACLE_HOME%\bin \crawlerlauncher.cmd contains the following line after the set `PATH=` line.

```
set TRUST_STORE_PATH=%WEBLOGIC_HOME%\server\lib\fusion_trust.jks
```

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

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

Settings for Oracle Fusion Applications Search with SSL Enabled on Linnux

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

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

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

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

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

Locking Down Web Services: Points to Consider

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

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

Service or Client Side	Internal Policy	Description
Service Side	`oracle/wss_saml_or_username_token_se`	The service accepts an unencrypted username and password token, or an unsigned Security Assertions Markup Language (SAML) token.
Client Side	`oracle/wss_username_token_client_poli`	The client sends an unencrypted username and password.
Client Side	`oracle/wss10_saml_token_client_policy`	The client sends unsigned SAML token.

These policies send and accept passwords in clear text, meaning unencrypted.. They do not perform any encryption or signing, and they do not have high security. However they are high performance because they don't do any expensive cryptography operations. They should be used only for backend Web services in small internal private networks that are completely blocked off from the internet and also blocked off from the enterprise intranet.

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

Service or Client Side	External Policy	Description
Service Side	`oracle/wss11_saml_or_username_token_`	The service accepts encrypted username and password token, or a signed SAML token, plus the entire message body must be signed and encrypted.
Client Side	`oracle/wss11_username_token_with_mes`	The client sends an encrypted username and password.
Client Side	`oracle/wss11_saml_token_with_message_`	The client sends signed SAML token.

`_policy`

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

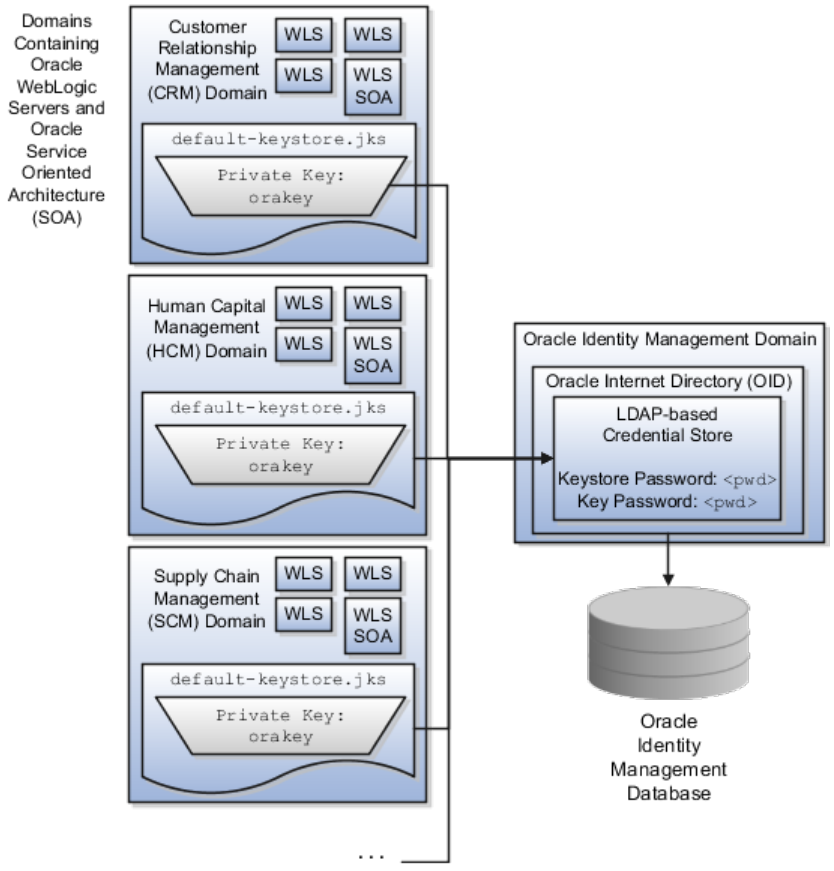
Oracle Fusion Applications provisioning also sets the following policies globally at the domain level.

Service or Client Side	Global Policy	Description
Service Side	`oracle/wss_saml_or_username_token_se`	The authentication only policy.
Client Side	`oracle/wss10_saml_token_client_policy`	The authentication only policy for SAML token.

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

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

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



Configuring External Clients to Communicate with Externally Facing Web Services

Since external Web services are protected by the external service `oracle/wss11_saml_or_username_token_with_message_protection_service_policy`,

external clients need to either provide username and password or a SAML assertion.

External clients must complete the following steps.

- Get the certificate of the service.

  The certificate is advertised in the Web Services Description Language (WSDL). To extract the certificate from the WSDL, perform the following steps.

  a. Save the WSDL to a local file.

  b. Search for the string `X509Certificate` inside the local file to locate the certificate.

     For example,

```
<dsig:X509Certificate> MIICHTCCAYagAwIBAgIETBwVYjA ... </
dsig:X509Certificate>
```

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

  d. Rename the file.

     1. If you are using this certificate in a Microsoft client, you can rename this file with .cer file extension and use it as a certificate file

     2. If you are using this certificate in a Java client, change the text file so that the certificate is framed by `BEGIN` and `END`.

        For example,

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

- Import the certificate of the service into your client's trust store.

  For Java clients use `keytool -importcert` to import this file from the previous step into your client's keystore.

- [For SAML only.] Generate a client certificate.

  If your client expects to perform ID propagation, the client needs to authenticate with SAML certificates. For this the client needs to have a client certificate for use as a SAML signing key

- [For SAML only.] Import the client certificate into the trust store of the service.

  Take the certificate in the previous step and import it into the default-keystore.jks file of the service.

Warning

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

Hardening Web Services

For more security you can make the following adjustments.

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

Caution

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

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

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

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

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

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

- You have set the SSL variables and client to go to OHS and then load balancer (LBR) if your SSL terminates at the LBR level.
- You have configured the policies for SAML Token (Sender Vouches) Over SSL for two-way SSL. Other authentication tokens such as username token, SAML bearer token, and so on, require only one-way SSL.

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

More Secure Keys and Certificates

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

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

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

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

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

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

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

Hardware Security Modules

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

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

3

Locking Down the Transactional Database with Advanced Security Features

Hardening the Transactional Database: Explained

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

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

Protecting Sensitive Data

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

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

Security Requirement	Hardening target	Hardening Reason	Security Feature
Protecting sensitive data at rest	Data beyond the PII defined by Oracle Fusion Applications	If access is gained to the file system or backups the data cannot be read.	Transparent Data Encryption Protecting sensitive data from DBAs
Protecting sensitive data from DBAs	Data beyond the PII defined by Oracle Fusion Applications	DBA access is not be subject to security policies in Oracle Platform Security Services (OPSS) and should therefore be limited or blocked through other means.	Oracle Data Vault and Oracle Audit Vault

Protecting sensitive data in clones	Data beyond the PII specified by the data masking templates defined in Oracle Enterprise Manager, integrated with Oracle Fusion Applications	Developers need realistic test data to test modifications and configurations. Such test data should be easy to construct, should test the real boundaries of the data, and should not allow developers to access information in the test environment that they would not be authorized to access in a live environment, except where there is a specific business reason for them to do so. Even when the data has been masked, access to it should be rigorously controlled, and all users made aware of their obligations and responsibilities with regard to it.	Oracle Data Masking
Protecting sensitive data in transit	Data beyond the PII protected by the enterprise deployment guidelines of Oracle Fusion Applications		Network security (instead or in addition to SSL)

Additional Data Protections

You can further secure the transmission of the data through mechanisms such as SSL or other network protections. You can use digital certificates to either encrypt or provide hash digests of the data prior to transmission to extend you defense-in-depth protections of private and sensitive data.

For partners who need a subset of production data, consider a dedicated data extract of only the data they need.

For more information about the advanced database security features, see the Oracle Database Advanced Security Administrator's Guide.

Data Encryption: Points to Consider

Encryption protects data as it is written to the file system against unauthorized access via that file system or on backups and archives. The data can be decrypted by applications when it is retrieved.

For information on the secure information life cycle in Oracle Fusion Applications, see the Oracle Fusion Applications Security Guide.

Transparent Data Encryption

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

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

Security Hardening Guidelines

As a security hardening guideline, use TDE at the level of tablespaces, which represents an optimal balance between performance and security.

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

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

You can view the list of encrypted tablespaces in Oracle Enterprise Manager. Enable tablespace level transparent data encryption on all Oracle Fusion Applications tablespaces

For information on enabling TDE on tablespaces, see the Oracle Database Advanced Security Administrator's Guide.

Data Management Hardening: Points to Consider

A vault hardens access controls such as privacy boundaries set by Oracle Virtual Private Database (VPD) from being overridden.

Oracle Database Vault

Oracle Database Vault (ODV) establishes limitations on the power of privileged users to access sensitive data through segregation of duties policies on database administrator (DBA) roles and by securely consolidating application data in the database. ODV lets you manage security for your database instance as a realm composed of the database or database objects that you want to secure. You can further secure the realm by creating rules, command rules, factors, identities, rule sets, and secure application roles.

Establishing the vault protects against insider threats, enforces separation of duties, and helps meets regulatory compliance requirements.

Security Hardening Guidelines

Using Oracle Database Vault Realms, you can enforce access to applications through a trusted path, preventing database users who have not been specifically authorized access from using powerful privileges to look at application data. For example, a database administrator (DBA)who has the SELECT ANY TABLE privilege can be prevented from using that privilege to view application data.

Define a single Oracle Fusion Applications Realm in Oracle Database Vault to protect all Fusion Applications schemas and objects.

Oracle Database Vault revokes the CREATE USER and other user management privileges from anyone who does not have the DV_ACCTMGR role.

For information about protecting application data from DBAs and other privileged users using Oracle Database Vault Realms, see the Oracle Database Vault Administrator's Guide.

For information about installing Oracle Database Vault on the existing ORACLE_HOME using Oracle Universal Installer and integrating it with such features as Transparent Data Encryption, see the Oracle Database Vault Administrator's Guide..

Data Masking: Points to Consider

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

Oracle Data Masking

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

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

For information about masking sensitive attributes in cloned databases, see the Oracle Enterprise Manager Concepts Guide.

Security Hardening Guidelines

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

The following entities are masked by Oracle Data Masking.

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

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

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

Offering	Masking Template
Customer Data Management	FUSION_CDM_VR1_Mask_Template.xml
Customer Relationship Management	FUSION_CRM_EXCEPT_CDM_TCA_VR1_Mask_Template.xml
Financials	FUSION_FIN_V1.0_Mask_Template.xml
Government Risk and Compliance	FUSION_GRC_VR1_Mask_Template.xml
Human Capital Management	FUSION_HCM_VR1_Mask_Template.xml
Procurement	FUSION_PRC_V1.0_Mask_Template.xml
Supply Chain Management	FUSION_SCM_VR1_Mask_Template.xml
Combined masking template for all product families	Combination_v1_ALL_Families.xml

The masking templates specify sensitive database tables and columns in Oracle Fusion Applications, and the data formats to be used to mask the columns. The masking templates provide examples as a starting point. They are not complete for all cases and can cause issues in how certain parts of the applications function.

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

Caution

As a security hardening guideline, clone the data needed for the set of tests in question, or at least truncate any tables containing sensitive data that are not

needed for the tests. Every piece of sensitive information that is cloned and not used represents an unnecessary risk.

4

Disabling Unused Components

Removing Unused Business Intelligence and Enterprise Performance Management Components: Explained

Components not in use in a deployment can represent unnecessary security risks.

Removing Debug Utilities in a Workspace Web Application

For troubleshooting purposes, Enterprise Performance Manager (EPM) Workspace is delivered with uncrunched JavaScript files. For security purposes, remove these uncrunched JavaScript files from your production environment.

1. Create a backup copy of `Oracle_BI1/common/epmstatic/wspace/js/directory`.
2. Delete all the `.js` files except `DIRECTORY_NAME` from each subdirectory of `Oracle_BI1/common/epmstatic/wspace/js`.

Each subdirectory contains a `.js` file that bears the name of the directory. For example, `Oracle_BI1/common/epmstatic/wspace/js/com/hyperion/bpm/web/common` contains `Common.js`. Remove all `.js` files except the one that bears the name of the directory, in this case, `Common.js`.

Disabling Operating System Services

Both UNIX and Windows platforms provide a variety of operating system services, most of which are not necessary for most deployments. Such services include FTP, TFTP, TELNET and so on. Be sure to close both the UDP and TCP ports for each service that is being disabled. Disabling one type of port and not the other does not make the operating system more secure.

Glossary

hardening

Process of securing a system by reducing its surface of vulnerability. Reducing available vectors of attack typically includes removing unnecessary software or unnecessary usernames or signins, deactivating unneeded features in configuration files, and disabling or removing unnecessary services.

offering

A comprehensive grouping of business functions, such as Sales or Product Management, that is delivered as a unit to support one or more business processes.

personally identifiable information

Any piece of information that can potentially be used to uniquely identify, contact, or locate a single person. Within the context of an enterprise, some PII data can be considered public, such as a person's name and work phone number, while other PII data is confidential, such as national identifier or passport number.