Oracle® Communications Order and Service Management

Security Guide

Release 7.3

E61815-01

July 2015

Oracle Communications Order and Service Management Security Guide, Release 7.3

E61815-01

Contents

4 Security Considerations for Developers

A Secure Deployment Checklist

Preface

This document describes Oracle Communications Order and Service Management (OSM) security considerations and procedures.

Audience

This document is intended for system administrators, system integrators, database administrators, and other individuals who are responsible for managing OSM and ensuring that the software is operating in a secure manner. This guide assumes that you have a working knowledge of OSM, the relevant operating system, Oracle Database, Oracle WebLogic Server, and Java J2EE software.

Downloading Oracle Communications Documentation

OSM documentation and additional Oracle documentation (such as database and WebLogic Server documentation) is available from the Oracle Help Center Web site:

`http://docs.oracle.com`

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support 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.

Related Documents

For more information about OSM security, see the following documents in the OSM documentation set:

- *OSM System Administrator's Guide*
- *OSM Installation Guide*

To implement security, OSM also uses other Oracle products, such as Oracle Database and WebLogic Server. See the following documents for more information about securing those products:

- *Oracle Database Security Guide*
- *Oracle Database Advanced Security Guide*
- *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*
- *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*

1 Overview

This chapter provides an overview of Oracle Communications Order and Service Management (OSM) security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols (such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL)), and secure passwords. See "Performing a Secure OSM Installation" for more information.
- **Learn about and use the OSM security features.** See "Implementing OSM Security" for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security. See "Security Considerations for Developers" for more information.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the Critical Patch Updates and Security Alerts Web site:

  `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`

Overview of OSM Security

OSM security is designed to protect application users, modules, solution data, order data, logs, and interfaces.

- **OSM application security:** Users of the application are authenticated using the Oracle WebLogic Server authentication framework.
- **OSM solution data security:** Solution data, such as deployed cartridges, is stored in the Oracle Database, which requires database credentials to access.

- **OSM order data security:** Application access to solution and order data is authorized and validated by the OSM role-based authorization model. Order data is stored in the Oracle Database, which requires database credentials to access.
- **OSM interface security:** Users of the application are authorized at the interface level (for example, Web client, Web service, or deployment) using the WebLogic Server security roles. Interfaces security is further configured using interface-specific means; the OSM Web service is secured by a WebLogic Server security policy, for example. Credentials for accessing external systems are stored securely.
- **Application log security:** Application log content is configured by users of the WebLogic Server **Administrators** group. The application distribution, settings and properties, and logs are protected by the user authorization and authentication procedures of the host operating system. Only the user who starts OSM has access to the files, based on file permissions.

  Note: The OSM server should be installed on a Windows-based computer only for development, demonstration, and (non-performance) test systems. Do not use a Windows-based system for production or performance test systems.

- **Database security:** The OSM database credentials are stored securely inside the Java Database Connectivity (JDBC) data source in the WebLogic server.

Understanding the OSM Environment

When planning your OSM implementation, consider the following:

- **Which resources need to be protected?**
  - You need to protect customer data.
  - You need to protect internal data.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.
- **Who are you protecting data from?**

  For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- **What will happen if protections on strategic resources fail?**

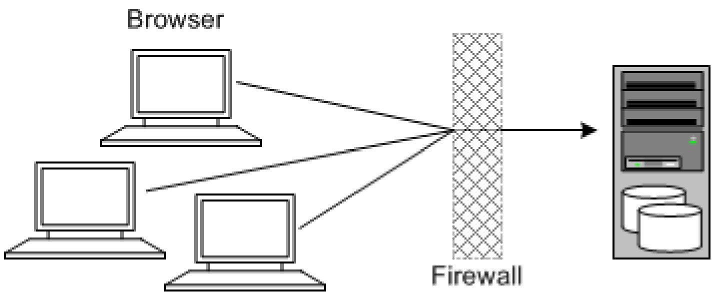
  In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Recommended Deployment Topologies

This section describes recommended deployment configurations for OSM.

Figure 1–1 shows a single-computer installation topology: the simplest OSM deployment architecture.

Figure 1–1 Single-Server Deployment Topology



In this topology, all the application components and data are kept on a single server, protected from external attacks by a firewall. The firewall can be configured to block known illegal traffic types. There are fewer resources to secure because all the components are on a single server and all of the communication is local. Fewer ports have to be opened through the firewall.

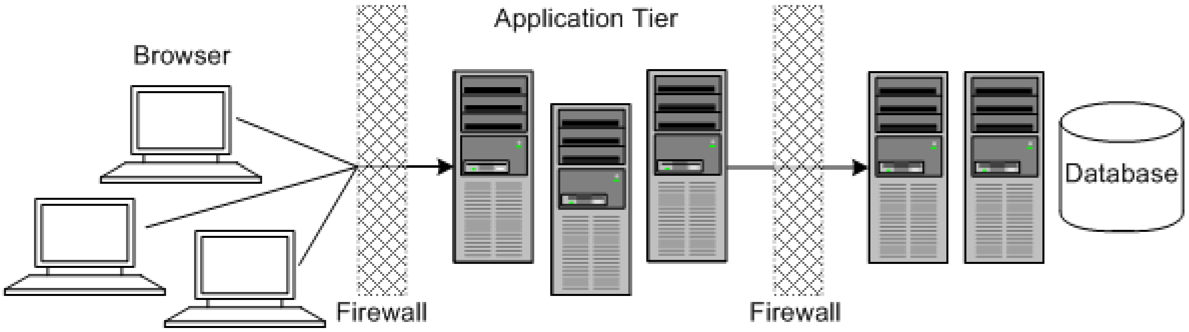
Conversely, there are fewer points of attack, and if security is compromised, an attacker would have access to the entire system and data.

A single-server installation topology is best suited for test and lab environments.

A single-server deployment is cost effective for small organizations but does not provide high availability because all components are stored on a single server.

Figure 1–2 shows a tiered installation deployment: a scalable OSM deployment offering greater security and high availability.

Figure 1–2 Tiered Deployment Topology



In this topology, the application tier is isolated by firewalls from both the Internet and the intranet. The database and servers are protected from potential attacks by two layers of firewall. Both firewalls can be configured to block known illegal traffic types. The two layers of firewall also provide intrusion containment. Although there are more components to secure, and more ports must be opened to allow secure communication between the tiers, the attack surface is spread out.

Operating System Security

This section describes operating system security topics that are specific to OSM. See the documentation for your operating system for general information.

Operating System Releases and Patch Levels

For information about the supported operating system releases and patch levels, see the system requirements in *OSM Installation Guide*. OSM depends on Oracle Database and WebLogic Server. For all operating systems, check the Oracle Database and WebLogic Server documentation for any additional operating system patches required to support those applications.

Restricting Permissions for OSM Directories

Oracle recommends keeping the permissions as restrictive as possible for your business needs. When installing on UNIX or Linux, consider using `umask 066` to deny read and write permission to all users except the user that installed the software. OSM creates files in the directories listed in Table 1–1. Examine these directories to ensure they have the appropriate permissions.

Table 1–1 OSM Directories

Name	Description
OSM home	The directory in which you installed OSM and all its subdirectories may be modified by OSM. This directory contains the **SDK** (if installed), **utility** (if installed), and product cartridge directories, as well as various installation-related files.
Domain home	The directory containing the WebLogic Server domain for OSM. The default location is *Fusion_Middleware_installation_directory***/user_projects/domains/***domain_name*, but it is frequently set to something else during installation.
VFS home	The directory in which OSM stores various solution files. The default location is **/tmp/vfs_cache**. If it is not using the default location, you will see the location in the value of the **-Djava.io.tmpdir=***new_path* argument to the OSM WebLogic Server startup scripts (where *new_path* is the parent directory of **vfs_cache**).

Port Security

OSM communicates over a limited number of ports. Depending on your solution requirements, additional ports may be required, especially if OSM is deployed to a WebLogic Server cluster.

Close all unused ports, especially non-SSL ports. Opt for SSL-enabled ports for all communications (for example: HTTPS or t3s) when possible.

The types of ports OSM uses are listed in Table 1–2.

Table 1–2 OSM Ports

Port	Port Description
Listen port for the administration server	The default value is 7001, but a different value can be set during domain creation.
SSL listen port for the administration server	The default value is 7002, but a different value can be set during domain creation.
WebLogic Server administration port (SSL-only)	The default value is 9001 if the administration port is enabled. By default, this port is disabled, but Oracle recommends enabling the port.
Coherence cluster port	The default value is 17001, but a different value can be set during OSM installation.

Table 1–2 (Cont.) OSM Ports

Port	Port Description
Database listener port	The default is 1521, but a different value can be set during database creation.

Oracle Database Security

This section describes database security topics specific to OSM. For more information about securing Oracle Database, see *Oracle Database Security Guide* and *Oracle Database Advanced Security Guide*. Some OSM database changes in this section must be made by an Oracle database administrator (DBA).

Oracle Database Administrator Roles and Permissions

The following roles and permissions are required for the account used by the DBA:

- Required permissions
  - Connect to a resource with admin option
  - Execute on dbms_lock with grant option
  - Execute on dbms_redefinition with grant option
  - Select on dba_jobs with grant option
  - Execute on exp_full_database and imp_full_database with admin option
  - Create table with admin option
  - Create materialized view with admin option
  - Query rewrite with admin option
  - Select on v_$parameter with grant option
- Required roles
  - sysdba role

Transparent Data Encryption

You can encrypt the OSM tablespace and schema, at the expense of system performance, using Oracle Database Transparent Data Encryption (TDE). Encrypting the schema and tablespace enforces data-at-rest encryption in the database layer and therefore prevents would-be attackers from bypassing the database and reading sensitive information from storage.

If you choose to encrypt the tablespace and schema, you must configure TDE on the tablespace before creating the OSM schema. See *Oracle Database Advanced Security Guide* for more information.

Dependent Schemas

Before creating the WebLogic Server domain, you must create certain database schemas using the Oracle Fusion Middleware Repository Creation Utility (RCU). For information about RCU, see *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*. For information about the RCU schemas required for creating an OSM WebLogic Server domain, see the information about installing and configuring WebLogic Server in *OSM Installation Guide*.

WebLogic Server Security

This section contains WebLogic Server security information relevant to OSM. For additional information about WebLogic Server security, see *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server* and *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*.

When planning your WebLogic Server domain installation, keep the following recommendations in mind:

- **Secure the WebLogic Server host:** WebLogic Server domain and server configuration files should be accessible only by the operating system users who configure or run WebLogic Server. No other operating system user (apart from the system administrators) should have read, write, or execute access to WebLogic Server product files or your domain files.
- **Set file access permissions for data stored in the persistent store:** Set operating system file access permissions to restrict access to data stored in the persistent store. When using the synchronous write policy of Direct-Write-With-Cache, limit access to the cache directory, especially if there are customized user access limitations on the primary directory. For more information about the WebLogic Server services and subsystems that can create connections to the persistent store, see the information about using the persistent store in *Administering Server Environments for Oracle WebLogic Server*. The default persistent store maintains its data in the *domain_home***/servers/***server_name***/data/store/default** directory, where *domain_home* is the home directory for the OSM domain, and *server_name* is the name of the relevant WebLogic server.
- **Do not run WebLogic Server in development mode in a production environment:** Production mode sets the server to run with settings that are more secure and appropriate for a production environment. For more information about development mode and production mode, see the information about domain modes in *Understanding Domain Configuration for Oracle WebLogic Server*.
- **Use appropriate encryption:** WebLogic Server includes a set of demonstration private keys, digital certificates, and trusted certificate authorities that are for development only; do not use the demonstration identity and trust in a production environment. See the topic on configuring keystores in the *Oracle WebLogic Server Administration Console Online Help* and the information about configuring SSL in *Administering Security for Oracle WebLogic Server* for more information about encryption.

  To prevent sensitive data from being compromised, secure data transfers by using HTTPS.

2

Performing a Secure OSM Installation

This chapter presents planning information for your Order and Service Management (OSM) installation.

For information about installing OSM, see *OSM Installation Guide*.

Pre-Installation Configuration

OSM depends on a database instance and Oracle WebLogic Server domain that have been properly configured. See "Operating System Security," "Oracle Database Security," and "WebLogic Server Security" for details on secure file system, database, and WebLogic Server domain configuration.

About the O7_DICTIONARY_ACCESSIBILITY Parameter

If you intend to use the **sys** user when the OSM installer prompts for database administrator credentials, you have two options:

- Ensure that the O7_DICTIONARY_ACCESSIBILITY parameter is set to **TRUE** in the database before running the OSM installer. If you choose this option, you should consider setting the parameter back to the default of **FALSE** after you have finished installing OSM.
- When prompted for the database administrator user name in the OSM installer, append **as sysdba** to the user name.

For more information, see the information about installing and configuring the database in *OSM Installation Guide*.

Installing OSM Securely

This section describes ways of ensuring that OSM is installed securely and information that you can use to secure installed components after installation.

Installation Type

You can perform a custom installation or a typical installation. Perform a custom installation to avoid installing options and products you do not need. If you perform a typical installation, remove or disable features that you do not need after the installation.

Password Policies

The OSM installer creates database schema and WebLogic Server domain application user accounts. The installer requires you to specify the password (and in some cases, user name) for these users. Oracle recommends the following password policies for these users, as well as users you create in the future:

- The password should be between eight and 24 characters long.
- The password should contain at least one letter, one number, and one special character.
- The password should not contain the user name.
- The user's account should be temporarily disabled after five login failures.

These recommended password policies are not implemented by default in the OSM installer, but should be configured manually after the installation. See *Oracle Database Security Guide* for information about implementing user security for Oracle Database users. For information about configuring the policies for WebLogic Server users, see the information about customizing the default security configuration in *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*.

Users and Groups

The OSM installer creates various users and groups in the database and in WebLogic Server. For information about the users and groups created by the OSM installer, see the information about installed components in *OSM System Administrator's Guide*.

The OSM installer creates the WebLogic Server users and groups listed in *OSM System Administrator's Guide*. If you intend to use another security implementation, such as LDAP, you must manually create those users and groups and assign the users to the groups.

Security-Relevant Installation Steps

Some steps in the installation process have security implications that you should keep in mind.

- In the WebLogic Server Connection Information window of the OSM installer, you can choose to connect to WebLogic Server over SSL, which encrypts all communications between the installer and the WebLogic administration server, including the user names and passwords that the installer creates.
- In the Order and Service Management Session Information window of the OSM installer, you can set the **Session Timeout** value for the OSM Web clients. It is a security risk to leave a session active for an extended period of time. Oracle recommends updating this setting to the lowest value that meets your business needs.
- In the Configuration Overview window of the OSM installer, you can choose to save the information you entered in the OSM installer to a configuration file, so that you can use it to perform a silent installation later. If you save the configuration, you also have the option of saving the passwords in the configuration file, but Oracle recommends that you do not select this option, because the passwords would be saved in plain text. If you are going to perform a silent installation, you should edit the file to enter the passwords immediately before running the silent installation and remove them when you are done.

3

Implementing OSM Security

This chapter provides a synopsis of the Order and Service Management (OSM) security features. For additional details, see the information about setting up OSM security in *OSM System Administrator's Guide*.

Secure Credential Management

OSM provides two distinct secure credential management solutions, each appropriate to the type of credential to be secured:

- **EncryptPasswords utility**: This utility is used to secure the credentials required to run other OSM utilities, such as the XML Import/Export tool. Oracle recommends that you use it when you run utilities unattended. If you are running the utilities attended, Oracle recommends that you provide the required credentials interactively as the utility prompted by the utility, rather than using EncryptPasswords. If you are using EncryptPasswords, must to be possible to perform an automated transformation of the password. Because the transformation of the password is automated, the output of EncryptPasswords should be considered obfuscated rather than encrypted. Secure the files containing the output with appropriate file-system-level restrictions.
- **Credential Store**: This utility is used to secure credentials required to access systems with which your OSM solution interacts. It builds on the Credential Store Framework (CSF), adding OSM-specific features.

For information about how to secure credentials using these methods, see *OSM System Administrator's Guide*.

Secure Solution Data Storage

As a fulfillment system, OSM does not need a fixed data model, and so is not required or typically used to store sensitive data other than that used for OSM user authentication.

You can secure OSM user credentials as described in "Secure Credential Management," but if your implementation requires OSM to store or log other sensitive data that appears on orders, Oracle recommends that you encrypt the data outside of OSM. Because the encryption happens outside of OSM, you are responsible for developing and maintaining the encryption method.

Using the WebLogic Scripting Tool

Several OSM features make use of the WebLogic Scripting Tool (WLST). When connecting to a WebLogic Server service instance, Oracle recommends that you connect to the service instance through the administration port. By default, this port is not enabled, but Oracle recommends that you enable the administration port in a production environment. The administration port requires all communication to be secured using SSL. By default, all servers in a WebLogic Server domain use demonstration certificate files for SSL, but these certificates are not appropriate for a production environment. For information about configuring the administration port, see the information about the administration port and administrative channel in *Administering Server Environments for Oracle WebLogic Server*. For more information about WLST, see *Oracle Fusion Middleware Understanding the WebLogic Scripting Tool*. For more information about connecting to WLST for OSM, see the information about managing and monitoring OSM in *OSM System Administrator's Guide*.

Secure Logging

OSM can be configured to suppress stack trace information in log output. A stack trace is a list of the method calls that an application is in the middle of at the time an exception is thrown. Running OSM with stack-trace logging enabled can be important for debugging the application during run time. However, in certain cases, suppressing this information can improve application security.

You can enable or disable logging stack traces using the **oms-config.xml** parameter **enable_log_stacktraces**. By default, this parameter is enabled. If there is a security concern about having log stack traces enabled, you can disable this parameter. For more information about setting this parameter, see the information about configuring OSM with **oms-config.xml** in *OSM System Administrator's Guide*.

4

Security Considerations for Developers

This chapter provides information for developers about how to create secure applications for Oracle Communications Order and Service Management (OSM), and how to extend OSM without compromising security.

Securely Communicating with External Systems

Securely communicating with an external system requires managing the following securely:

- the credentials required to access the system
- the communication between OSM and the external system

You store credentials securely by using the OSM secure credential storage feature, described in "Secure Credential Management."

For reliability, Oracle recommends that communication with external systems be over Java Messaging Service (JMS). OSM creates a JMS module, **oms_jms_module**, for this purpose, which is secured from unauthorized access. Only members of the following Oracle WebLogic Server groups are allowed access to resources created in this module:

- **OMS_client**
- **OMS_ws_api**
- **OMS_xml_api**
- **OSM_automation**
- **Cartridge_Management_WebService**

See the information about installed components in *OSM System Administrator's Guide* for additional information about the OSM WebLogic Server groups. Oracle recommends that any other JMS modules with which OSM interacts be similarly configured. Ensure that the associated persistent store is properly secured, as described in "WebLogic Server Security."

Security Callback

OSM allows developers to add additional authorization and auditing to the default order data access model. For information on where and how this feature may be leveraged, see the information about using OSM security callback in *OSM Developer's Guide*.

Hiding Sensitive Data in the Web Client

You can ensure that the OSM Web clients obscure OSM solution data by identifying that the data is secret at design time. A data node declared as secret in Oracle Communications Design Studio is rendered as a password field in the OSM Web clients. For more information, see *Modeling OSM Processes* Help.

Web Service Security

Access to the OSM Web services is restricted to members of the **OMS_ws_api** WebLogic Server group. Access to specific operations, such as CreateOrder, CancelOrder, and UpdateOrder, are further restricted through OSM role and order life cycle policy permissions. For information about OSM roles and order life cycle policies, see *Modeling OSM Processes* Help.

A

Secure Deployment Checklist

The following security checklist lists guidelines to help you secure Oracle Communications Order and Service Management (OSM) and its components.

- Install only the components you need.
- Enforce strong password management.
- Restrict and control user privileges.
- Restrict network access by doing the following:
  - Use firewalls.
  - Never leave an unnecessary opening in a firewall.
  - Monitor who accesses your systems.
  - Encrypt network traffic.
  - Install the operating system in a secure location that is difficult for a hacker to access.
- Apply all security patches and workarounds.
- Encrypt sensitive information.
- Contact Oracle support if you discover a vulnerability in any Oracle product.