

Oracle Thesaurus Management System

Security Guide



Release 5.3.1
F51281-01



Copyright © 1996, 2022, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Documentation accessibility	v
Diversity and Inclusion	v
Related resources	v
Access to Oracle Support	v

1 Security Guide

Introduction	1-1
General Security Principles	1-2
Restrict Network Access to Critical Services	1-2
Monitor System Activity	1-2
Set Up a Change Management Process	1-2
Change Passwords Periodically	1-3
Keep Passwords Private and Secure	1-3
Use Profiles	1-3
Lock Computers to Protect Data	1-3
Close All Open Ports Not in Use	1-3
Secure the Environment	1-3
Provide Only the Necessary Rights to Perform an Operation	1-3
Secure Installation and Configuration	1-4
Install Critical Patch Updates (CPUs) and Critical Patch Set	1-4
Use SSL (HTTPS) Between Browser and Web Server	1-4
Signed Certificates for HTTPS	1-4
Disable Unused Services	1-5
Replace Verbose Errors with Custom Messages	1-5
Secure the WebLogic Server	1-5
Provide Security for Session-Tracking Cookies	1-5
Provide Security for Cross-Frame Scripting	1-6
Configure Strong Passwords on the Database	1-6
Hide Oracle Forms Version Numbers	1-7
Secure the Reports Server	1-7
Application Security Features	1-7

Secure the Reports Server	1-7
TMS Security	1-7
Use Data Access Groups to Restrict Access to the Application	1-7
Enforce Password Security	1-8
Database Roles and Menu-Based Security	1-8

Preface

This preface contains the following sections:

- [Documentation accessibility](#)
- [Diversity and Inclusion](#)
- [Related resources](#)
- [Access to Oracle Support](#)

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>.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related resources

All documentation and other supporting materials are available on the [Oracle Help Center](#).

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through Support Cloud.

Contact our Oracle Customer Support Services team by logging requests in one of the following locations:

- English interface of Oracle Health Sciences Customer Support Portal (<https://hsghbu.custhelp.com/>)
- Japanese interface of Oracle Health Sciences Customer Support Portal (<https://hsghbu-jp.custhelp.com/>)

You can also call our 24x7 help desk. For information, visit <http://www.oracle.com/us/support/contact/health-sciences-cloud-support/index.html> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

1

Security Guide

This guide describes essential security management options for Oracle Thesaurus Management System (TMS) Release 5.3.x.

- [Introduction](#)
- [General Security Principles](#)
- [Secure Installation and Configuration](#)
- [Application Security Features](#)

Introduction

This security guide provides guidelines and recommendations for installing, configuring, and monitoring Oracle TMS to make them more secure in customer environments. This is a practical guide for technical users, installers, and system administrators who implement and maintain the Oracle TMS system. This document discusses guidelines for hardening of the Oracle TMS security application, and other system hardening configuration recommendations.

This document cannot address every security scenario that might be applicable to a particular implementation and environment; however, it provides basic recommendations for securing Oracle TMS. Oracle recommends that you fully test the security setup in a non-production environment to ensure proper functionality and integrity before you install the software.

This guide will help you ensure that Oracle TMS and the various components involved in the setup are properly secured. Oracle recommends that you secure the Oracle TMS environment in alignment with your company's enterprise security policies.

This guide is not intended to replace the Oracle TMS technical documentation (Installation Guide and User's Guide) delivered with the product. It provides references to relevant information in Installation and User's Guides. Readers of this guide should have a good understanding of Oracle TMS. Implementing Oracle TMS security requires an in-depth understanding of many disciplines, including WebLogic Server administration, Oracle Database security administration, and network security administration.

This guide presents the following security guidelines and recommendations:

- [General Security Principles](#)
- [Secure Installation and Configuration](#)
- [Application Security Features](#)

In addition, see the following documents for security configuration instructions:

- *Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server*
- *Oracle Fusion Middleware Securing Oracle WebLogic Server*
- *Oracle Fusion Middleware Information Roadmap for Oracle WebLogic Server*
- *Oracle Application Server Web Services Security Guide*

General Security Principles

This section provides general security recommendations for securing any application.

The most critical resource to protect is the Oracle TMS database, which contains information that is both sensitive and critical to the performance of your business. Oracle recommends that you protect most of your computing resources from unauthorized access, manipulation, or destruction from both internal and external parties.

For Web enablement, you must protect resources from unauthorized access via the Internet. In addition, access to highly confidential data or strategic resources should be available to only a few trusted users or system administrators.

This section includes:

- [Restrict Network Access to Critical Services](#)
- [Monitor System Activity](#)
- [Set Up a Change Management Process](#)
- [Change Passwords Periodically](#)
- [Keep Passwords Private and Secure](#)
- [Use Profiles](#)
- [Lock Computers to Protect Data](#)
- [Close All Open Ports Not in Use](#)
- [Secure the Environment](#)
- [Provide Only the Necessary Rights to Perform an Operation](#)

Restrict Network Access to Critical Services

Oracle recommends that you install a firewall between the database and application servers. In addition, if you are using Web Tier, consider placing a firewall between the Oracle HTTP Server (OHS) and the WebLogic Server. The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls.

Monitor System Activity

One of the main requirements of system security is monitoring. Auditing and reviewing audit records address this requirement. Each component within a system has some degree of monitoring capability. Oracle recommends that you establish a policy to check and monitor activities in your system regularly. Refer to the database and application server documentation for audit functionality.

Set Up a Change Management Process

Oracle recommends that you establish a policy to set up a change management process to keep track of all the changes in your software systems. All changes to software should be approved and audited.

Change Passwords Periodically

It is good practice to change both system account passwords and user passwords periodically. Follow your organization's operating procedures for the frequency of making changes.

Keep Passwords Private and Secure

All users should change their passwords when they log in for the first time.

Tell users never to share passwords, write down passwords, or store passwords in files on their computers.

Encourage users to choose password-reset questions and answers that are easy for them to remember, but difficult for someone else to guess.

Use Profiles

In the Oracle database, a profile is a named set of resource limits and password parameters that restrict database usage and instance resources for a user. By default, every Oracle TMS user is assigned the DEFAULT profile. You can change its limitations on resources or password use or assign a separate profile to each user or user role. Each user can have only one profile. For more information, see the *Oracle Thesaurus Management System Installation Guide* and the *Oracle Database Security Guide*.

Lock Computers to Protect Data

Encourage users to lock computers that are left unattended.

Close All Open Ports Not in Use

Keep only the minimum number of ports open. You should close all ports not in use.

Secure the Environment

To ensure security in the Oracle TMS application, carefully configure all components, including the following third-party components:

- Web browsers
- Firewalls
- Load balancers
- Virtual Private Networks (VPNs)

For more information, see the documentation for the application you are configuring.

Provide Only the Necessary Rights to Perform an Operation

Assign database roles or custom roles so that users can perform only the tasks necessary for their jobs.

Secure Installation and Configuration

This section provides information for securely installing and configuring the Oracle TMS application, including but not limited to configuring firewall settings, installing signed certificates when using HTTPS, and closing unused ports.

This section includes:

- [Install Critical Patch Updates \(CPUs\) and Critical Patch Set](#)
- [Use SSL \(HTTPS\) Between Browser and Web Server](#)
- [Signed Certificates for HTTPS](#)
- [Disable Unused Services](#)
- [Replace Verbose Errors with Custom Messages](#)
- [Secure the WebLogic Server](#)
- [Provide Security for Session-Tracking Cookies](#)
- [Provide Security for Cross-Frame Scripting](#)
- [Configure Strong Passwords on the Database](#)
- [Hide Oracle Forms Version Numbers](#)
- [Secure the Reports Server](#)

Install Critical Patch Updates (CPUs) and Critical Patch Set

To ensure that your installation includes up-to-date security fixes, install the latest Oracle CPUs and critical patch set.

For more information, see the *Oracle Thesaurus Management System Installation Guide*.

Use SSL (HTTPS) Between Browser and Web Server

Information sent over the network and across the Internet in clear text may be intercepted. Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) are features that provide encryption of network traffic between the browser and the Oracle TMS web server.

For more information, see the *Oracle Thesaurus Management System Installation Guide*.

Signed Certificates for HTTPS

To support HTTPS for Oracle TMS, you need to request a signed certificate from a Certificate Authority (CA) vendor such as Thawte or Verisign, and then import the signed certificate into the Oracle Wallet for the Oracle Application Server.

For more information, see the *Oracle Thesaurus Management System Installation Guide*.

Disable Unused Services

The Oracle TMS application does not use the following services or information for any functionality:

- **Simple Mail Transfer Protocol (SMTP).** This protocol is an Internet standard for e-mail transmission across Internet Protocol (IP) networks.
- **Identification Protocol (identd).** This protocol is generally used to identify the owner of a TCP connection on UNIX.
- **Simple Network Management Protocol (SNMP).** This protocol is one method for managing and reporting information about different systems.

Therefore, restricting these services or information will not affect those Oracle applications. If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure.

If you need SMTP, identd, or SNMP for other applications, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

In addition, Oracle recommends that you remove unused Oracle TMS user accounts if you are upgrading from earlier releases.

Replace Verbose Errors with Custom Messages

Web applications issue HTTP error messages, such as Error Code 500 (Internal Server Error) and Error Code 404 (Not Found), for servlet exceptions that occur at run time (for example, when a servlet is processing the form data). Some internal error messages are verbose and provide sensitive system information.

To tighten the security on your production systems, Oracle recommends that you replace the verbose error messages with brief customized messages.

You can create an HTML error page containing a custom message, and then use the XML error-page element and subelements in the web.xml file to specify the HTML error page to use for the servlet exceptions. You can create a different error message for each error number or use the same generic message for more than one error.

Oracle recommends that you edit the web.xml file for the Oracle TMS application.

Secure the WebLogic Server

For information on securing the WebLogic Server, see:

- *Oracle Fusion Middleware Securing Oracle WebLogic Server*
- *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*
- "Security" in *Oracle Fusion Middleware Information Roadmap for Oracle WebLogic Server*

Provide Security for Session-Tracking Cookies

You can use the XML session-tracking element to provide security for the TMS Lite Browser session-tracking cookies.

In the `orion-web.xml` file, you can configure the following flags (attributes) for the session-tracking element:

- **set-secure** — Requests that your Internet browser only honor the HTTPS protocol to access Web sites. If you set the secure flag to **true**, users must enter `https://` to access Web sites. Entering `http://` will not work.
- **HttpOnly** — Requests that your Internet browser honor only the HTTP and HTTPS protocols to access Web sites. Other protocols, such as FTP, will not work.

 **Note:**

If you configure the secure and HttpOnly flags for session-tracking cookies, you must make the changes on all servers in a load-balanced environment.

Once you complete the above changes, access to the application using HTTP will not work. Users will be forced to use HTTPS only.

Provide Security for Cross-Frame Scripting

You can enable Oracle HTTP Server to send Content-Security-Policy "frame-ancestors" for all the TMS request.

1. Edit the `httpd.conf` file located under `<FRDomain_Home>\config\fmwconfig\components\OHS\ohs1\` and `<FRDomain_Home>\config\fmwconfig\components\OHS\instances\ohs1\`.
2. Add the following in the `httpd.conf` file:

```
<Location /tmsadf>
  <IfModule mod_headers.c>
    Header set Content-Security-Policy "frame-ancestors 'self';"
  </IfModule>
</Location>
```

3. Restart the OHS instance.

TMS is implementing the ADF security recommendations for Cross-Site Scripting and ADF sends the X-Frame-Options Sameorigin header for the request, as needed.

Configure Strong Passwords on the Database

Although the importance of passwords is well known, the following basic rule of security management is worth repeating:

Ensure all your passwords are strong passwords.

You can strengthen passwords by creating and using password policies for your organization.

You should modify the following passwords to use your policy-compliant strings:

- Passwords for the database default accounts, such as SYS and SYSTEM.
- Passwords for the database application-specific schema accounts, such as RXC, OPA, and RXC_PD. You can run the Set Password (`set_pwd`) utility to set stronger

passwords for the default Oracle TMS schemas. For details on using the utility, refer to the *Oracle Thesaurus Management System Installation Guide*.

- Password for the database listener. If you do not configure the database listener to require an authorization password, you unnecessarily expose the underlying database service names to unauthorized individuals.

For guidelines on securing passwords and for additional ways to protect passwords, refer to the *Oracle Database Security Guide* specific to the database release you are using.

Hide Oracle Forms Version Numbers

By default, the current version of Oracle Forms is displayed when someone accesses a forms servlet URL. This is because the form parameter in formsweb.cfg calls test.fmx, which displays the version number so that you can check the version you are running.

To change this behavior:

1. Create a new file based on test.fmx that does not display the version number.
2. In formsweb.cfg, default section, set form=*your_new_file*.

Secure the Reports Server

See My Oracle Support note *Secure the Showjobs Web Command in a Non Secured Reports Server in Oracle Reports 11g*, ID 1242614.1.

Application Security Features

This section includes:

- [Secure the Reports Server](#)
- [TMS Security](#)

Secure the Reports Server

See My Oracle Support note *Secure the Showjobs Web Command in a Non Secured Reports Server in Oracle Reports 11g*, ID 1242614.1.

TMS Security

This section provides information for securing the TMS application, users, and data.

- [Use Data Access Groups to Restrict Access to the Application](#)
- [Enforce Password Security](#)
- [Database Roles and Menu-Based Security](#)

Use Data Access Groups to Restrict Access to the Application

In TMS, database roles dictate which windows in the user interface a user can access. For users assigned to one or more Data Access Groups (DAGs), their assignments dictate the data they see in TMS windows and in the HTML Browser, and whether or not they can operate on TMS data in specific dictionaries and/or domains. You define DAGs in the Maintain DAGs window and then assign users to the group either in the User Assignments

tab of the Maintain DAGs window or as you create user accounts. For more information, see the *Oracle Thesaurus Management System User's Guide*.

Enforce Password Security

Each password should meet or exceed the minimum requirements for the application. For example, a password may need to:

- Contain a minimum of eight characters.
- Contain at least one upper case character, and one alphanumeric character.

For more information, see the documentation for the application you are configuring.

Oracle enables a database administrator to enforce various rules about passwords at the database level, including setting a password lifetime, after which users must set a new password; disallowing reuse of previous passwords; locking an account after a user attempts to log on a specified number of times; and creating complexity rules for passwords through a PL/SQL function. For more information, see the *Oracle Thesaurus Management System Installation Guide*.

Database Roles and Menu-Based Security

TMS includes predefined roles that you can assign to users. A predefined role determines the functions and menu options that are available to a user. You can enforce security by assigning users only the database roles they need to do their work, preventing them from seeing other parts of the system and taking actions they are not authorized to take.

You can also create custom database roles, which may be required if the database roles that are supplied as part of the installation do not fit or cannot be modified to fit your business model.

For more information, see the *Oracle Thesaurus Management System User's Guide*.