Oracle Argus Mart

Minimum Security Configuration Guide

Release 8.4
F51786-01
September 2022

Oracle Argus Mart Minimum Security Configuration Guide, Release 8.4

F51786-01

Contents

Preface

This preface contains the following sections:

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.

Related resources

For information about Oracle Argus patches, see My Oracle Support.

All documentation and other supporting materials are available on the Oracle Help Center.

Access to Oracle Support

To receive support assistance, determine whether your organization is a cloud or on-premises customer. If you're not sure, use Support Cloud.

Cloud customers receive support assistance through Support Cloud

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://hsgbu.custhelp.com/)
- Japanese interface of Oracle Health Sciences Customer Support Portal (https://hsgbu-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.

On-premises customers receive support assistance through My 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.

1

Minimum Security Configuration Guide

This guide describes essential security management guidelines and recommendations for the Oracle Argus Mart application. It contains the following topics:

Keep up to date on software and latest Critical Patch Updates

Oracle continually improves its software and documentation. Critical Patch Updates are the primary means of releasing security fixes for Oracle products to customers with valid support contracts.

Oracle highly recommends that customers:

- Keep all software versions and patches up to date.
- Apply Critical Patch Updates as soon as they are released.

Establish SQLPLUS Connection

To connect to SQLPLUS, execute the following steps:

1. Open a command prompt in Windows.

   Alternatively, in Unix, type at the shell prompt.
2. Enter the *sqlplus <dbuser>@<tnsnames_entry>* command, and press **Enter**.
3. Enter the password when prompted by the SQLPLUS program.

   You must not enter the password in the same command line that is used while calling the SQLPLUS program.

Configure Strong Password on the Database and WLS

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

Make sure all your passwords are strong passwords.

You can strengthen passwords by creating and using password policies for your organization. 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.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 weblogic server default accounts, such as weblogic.
- 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.

Close All Open Ports not in Use

Keep only a minimum number of ports open. You should close all ports that are not in use.

Disable the Telnet Service

The Oracle Argus Mart application does not use the Telnet service. Telnet listens on port 23 by default. If the Telnet service is available on the Oracle Argus Mart host machine, Oracle recommends that you disable Telnet in favor of Secure Shell (ssh). Telnet, which sends clear-text passwords and user names through a login, is a security risk to your servers. Disabling Telnet tightens and protects your system security.

Disable Other Unused Services

In addition to not using Telnet, the Oracle Argus Mart 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 the Oracle Argus Mart application. 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.

(Optional) Encrypt Tablespaces using the Oracle Advanced Security TDE

Oracle Database Transparent Data Encryption (TDE) feature is part of the Oracle Advanced Security option available for Oracle Database Enterprise Edition 19c, see https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/asopart1.html.

TDE provides the capability to encrypt sensitive data in the Oracle Database in a manner that is transparent to applications.

Oracle Argus Mart product has been functionally certified with tablespace level encryption using the Oracle Database TDE feature.