Oracle® Argus Mart

Minimum Security Configuration Guide

Release 8.1.1

E88813-01

September 2017

This guide describes essential security management options for the Oracle Argus Mart application.

1 Introduction

This guide presents the following security guidelines and recommendations:

- Establishing SQLPLUS Connection
- Configuring Strong Password on the Database and WLS
- Closing All Open Ports not in Use
- Disabling the Telnet Service
- Disabling Other Unused Services

2 Establishing 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 s*qlplus <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.

3 Configuring 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.

4 Closing All Open Ports not in Use

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

5 Disabling the Telnet Service

The Argus Mart application does not use the Telnet service. Telnet listens on port 23 by default.

If the Telnet service is available on the 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.

6 Disabling Other Unused Services

In addition to not using Telnet, the 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 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.

7 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.

Oracle Argus Mart Security Configuration Guide, Release 8.1.1
E88813-01