

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 `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.

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.

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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.

