

Oracle® Virtual Operator Panel
Security Guide

E48643-02

March 2014

Oracle Virtual Operator Panel Security Guide

E48643-02

Copyright © 2013, 2014, 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, 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 on 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. 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.

Contents

1 Overview

| | |
|----------------------------------|-----|
| Product Overview..... | 1-1 |
| General Security Principles..... | 1-1 |

2 Secure Installation and Configuration

| | |
|--|-----|
| Installation Overview..... | 2-1 |
| Understand Your Environment | 2-1 |
| Installing Oracle Virtual Operator Panel | 2-1 |
| Post Installation Configuration..... | 2-1 |
| Change Default Passwords..... | 2-1 |
| Enforce Password Management | 2-1 |

3 Security Features

| | |
|-------------------------|-----|
| The Security Model..... | 3-1 |
|-------------------------|-----|

A Secure Deployment Checklist

B Open Ports

C References

Preface

This document describes the security features of Oracle's Virtual Operator Panel.

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of Oracle's Virtual Operator Panel.

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 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.

This section gives an overview of the product and explains the general principles of application security.

Product Overview

Oracle's Virtual Operator Panel is a suite of Java applications that provide a graphical user interface for managing tape drives. Customers and service engineers use Virtual Operator Panel to view, set or modify configuration parameters, display or monitor status, and perform diagnostics, troubleshooting, and service tasks (for example, download firmware).

General Security Principles

The following principles are fundamental to using any application securely:

- **Keep Software Up To Date**

One of the principles of good security practice is to keep all software versions and patches up to date. Throughout this document, we assume Oracle Virtual Operator Panel version of 2.0 or later.
- **Restrict Network Access**

Keep the Oracle Virtual Operator Panel application behind a firewall, in a secure, data center environment. Also, if possible, it is preferable to install the Oracle Virtual Operator Panel application on a server on a private LAN. The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. The Oracle Virtual Operator Panel application is not designed to have public or internet access.
- **Follow the Principle of Least Privilege**

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. User privileges should be reviewed periodically to determine relevance to current job responsibilities.
- **Monitor System Activity**

System security stands on three legs: good security protocols, proper system configuration and system monitoring. Auditing and reviewing audit records address this third requirement.
- **Keep Up To Date on Latest Security Information**

Oracle continually improves its software and documentation. Check this note yearly for revisions.

Secure Installation and Configuration

This section provides Oracle Virtual Operator Panel application security as it relates to installation and configuration.

Installation Overview

This section outlines the planning process for a secure installation.

Understand Your Environment

Oracle Virtual Operator Panel is intended to be used in a secure environment. Be sure to install on computers, and in networks, that are in a secure environment, for both physical access and network access.

Installing Oracle Virtual Operator Panel

For more information about installing Oracle Virtual Operator Panel, refer to the *Oracle Virtual Operator Panel User's Guide*.

Post Installation Configuration

This section describes security configuration changes that must be made after installation.

Change Default Passwords

Security is most easily broken when a default user account still has a default password even after installation

Enforce Password Management

Apply basic password management rules, such as password length, history, and complexity, to all user passwords.

Security Features

This section outlines security mechanisms offered by Oracle Virtual Operator Panel.

The Security Model

Because the intended environment for Oracle Virtual Operator Panel is a secure, data center environment, the security model is minimal, and depends on the computer and network being physically secure.

For legacy tape drives (for example, StorageTek 9840D, T10000C, IBM LTO5, HP LTO5, and earlier) the protocols used are telnet (port 23) and FTP (port 20, 21), which are unencrypted.

Beginning with this release (VOP 2.0), and future drives which support it, SSH and SFTP are the defaults.

Secure Deployment Checklist

Ensure that you do the following:

- Keep Oracle Virtual Operator Panel and the tape drives it manages behind the corporate firewall.
- Harden the Solaris or Linux operating system.
- Apply all security patches and workarounds.
- Contact your Oracle Services, Oracle Tape Library Engineering, or account representative if you come across vulnerabilities in Oracle tape drives.

Open Ports

The following lists the default ports that might be open on Oracle Virtual Operator Panel:

Port: 22

- Protocol: TCP
- Service: SSH
- Open by Default? Yes



C

References

You can access Oracle Virtual Operator Panel user documentation from the Oracle Technical Network (OTN) Tape Storage Products page:

<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html>

