

Oracle® StorageTek Virtual Operator Panel

Security Guide

2.0

E37312-01

September 2012

Oracle StorageTek Virtual Operator Panel Security Guide 2.0

E37312-01

Copyright © 2012, Oracle and/or its affiliates. All rights reserved.

Primary Author: Andy Hewitt

Contributors: VOP Development Team

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 software or related documentation 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 RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software

License (2012). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software 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

Part 1: Overview	4
Product Overview.....	4
Keep Software Up To Date.....	5
Restrict Network Access	5
Follow the Principle of Least Privilege	5
Monitor System Activity	5
Keep Up To Date on Latest Security Information	5
Part 2: Secure Installation and Configuration.....	6
Installation Overview	6
Understand Your Environment.....	6
Installing VOP	6
Post Installation Configuration.....	6
Part 3: Security Features.....	7
The Security Model	7
Part 4: Appendices.....	8
Appendix A: Secure Deployment Checklist.....	8
Appendix B: Open Ports	9
References	10
VOP Documentation.....	10

Part 1: Overview

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

Product Overview

Oracle's StorageTek Virtual Operator Panel (VOP) is a suite of Java applications that provide a graphical user interface for managing tape drives. It is used by customers and service engineers 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 VOP version of 2.0 or later.

Restrict Network Access

Keep VOP application behind a firewall, in a secure, data center environment. Also, if possible, it is preferable to install VOP 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. *Note: VOP 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.

Part 2: Secure Installation and Configuration

Installation Overview

This section outlines the planning process for a secure installation.

Understand Your Environment

VOP 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 VOP

For more information about installing VOP see StorageTek Virtual Operator Panel User's Guide (Part Number: E37053-01).

Post Installation Configuration

In this section document any security configuration changes that must be made after installation.

Change default user 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.

Part 3: Security Features

In this section outline the specific security mechanisms offered by the product.

The Security Model

Because the intended environment for VOP is a secure, data center environment, the security model for VOP 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.

Part 4: Appendices

Appendix A: Secure Deployment Checklist

1. Keep VOP and the tape drives it manages behind the corporate firewall.
2. Harden the Solaris or Linux operating system.
3. Apply all security patches and workarounds.
4. Contact Oracle Support if you come across vulnerability in Oracle VOP.

Appendix B: Open Ports

The following table lists the default ports that might be open on [VOP].

Port	Protocol	Service	Open by Default?
22	TCP	SSH	Yes

References

VOP Documentation

The VOP documentation is saved in libraries organized by VOP release. Access this from [Tape Storage Documentation page](#).