# StorageTek T10000

Security Guide for T10000A/B/C

Release 2

**E28826-02**

April 2013

ORACLE

StorageTek T10000 Security Guide, Release 2

E28826-02



Primary Author: Dave Hostetter

Contributing Author:

Contributor:

# Contents

# Preface

This document describes the security features of Oracle's StorageTek T10000.

## Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of StorageTek T10000.

## 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.

# 1

# Overview

This section gives an overview of the T10000A/B/C tape drives and explains the general principles of tape drive security. This security guide covers the T10000A, T10000B, and T10000C tape drives.

## Product Overview

The T10000A/B/C family of Enterprise tape drives attach to both open systems SCSI over Fibre Channel protocol and to mainframe over FICON protocol. The T10000 tape drives transfer data to and from a host and stores it on a removable magnetic media. The T10000 family of tape drives intend primarily to provide high reliability, high capacity back up, archive, and data processing capabilities for enterprise customers that demand high duty cycle and reliability. Each product in the family provides optional data encryption. The customer has the option to enable the encryption feature. All products meet the minimum Federal Information Processing Standard (FIPS 140-2 Level 1). Each tape drive product was enhanced for capacity and native tape speed. In addition, data management features were also added along the way. The following describes the capacity and performance migration from one generation to the next.

**T10000A**
500 GB capacity and 120 MB per second native tape speed

**T10000B**
1TB capacity and 120 MB per second native tape speed

**T10000C**
5TB capacity and 240 MB per second native tape speed

## Security

All tape drive products are designed and documented for use within a controlled hardware environment. Tape Drives are always located inside a controlled data center and they are typically located inside of a Tape Library. In some cases the customer will use a rack mount version but that is rare. The controlled data center is also inside a fire wall that is protected by the customer's own security policies. This will give the best functionality and protection from compromise, both from the internet in general and from the internal entity operating the tape drive.

## General Security Principles

The following principles are fundamental to using any product 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 software level of:

T10000A 1.48.112
T10000B 1.48.212
T10000C 1.53.316 (released on September 2012)
T10000C 1.57.308 (released on April 2013)

## Restrict Network Access

Keep the tape drive behind a data center firewall. The firewall provides assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls. It is recommended that you identify the hosts allowed to attach to the Tape Drive and block all other hosts if possible.

## Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check this document every release for revisions.

# 2

# Secure Installation

This section outlines the planning and implementation process for a secure installation and configuration, describes several recommended deployment topologies for the systems, and explains how to secure a tape library.

## Understand Your Environment

To better understand security needs, the following questions must be asked:

### Which resources need to be protected?

Many resources in the production environment can be protected. Consider the resources needing protection when deciding the level of security that must provided.

### From whom are the resources being protected?

The tape drive must be protected from everyone on the Internet. But should the tape drive be protected from the employees on the intranet in your enterprise?

### What will happen if the protections on strategic resources fail?

In some cases, a fault in a security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use the tape drive. Understanding the security ramifications of each resource will help protect it properly.

## Securing the Tape Drive

By default, the Tape Drive uses ports listed in the following table. The firewall should be configured to allow traffic to use these ports and that any unused ports are blocked. The Tape Drives support IPv6 and IPv4.

***Table 2–1 Network ports used***

| Port | T10000A | T10000B | T10000C |
|---|---|---|---|
| 22 tcp - SSH VOP | | | |
| 22 tcp - SFTP | | | |
| 161 udp - SNMPV1 Tape Drive agent requests - inbound stateful | X | X | X |

*Table 2–1 (Cont.) Network ports used*

| Port | T10000A | T10000B | T10000C |
|---|---|---|---|
| 162 udp - SNMPV1 Tape Drive traps and inform notifications - outbound stateless for traps, outbound stateful for inform | X | X | X |
| 23 tcp - TELNET | X | X | X |
| 21 tcp - FTP | X | X | X |
| 9842 tcp - EPT | X | X | X |
| 3331 OKM - challenge and root CA service | X | X | X |
| 3332 OKM – Enrollment. Cyber strength is AES256 | X | X | X |
| 3334 OKM – Encryption key exchange. Cyber strength is AES256 | X | X | X |
| 3335 OKM – Cluster discovery. Cyber strength is AES256 | X | X | X |

# Installing Virtual Operator Panel (VOP) application

VOP should only be installed on systems that are within the same protected network infrastructure as the tape drive. Customer access controls should be enforced on the systems where VOP is installed to assure restricted access to the tape drive. See Table 2–1 for ports used by VOP.

Refer to the following VOP user guide for web launch VOP install instructions.

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#vop

# Post Installation Configuration

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

## Assign the user (admin) password.

The customer admin account password should be changed by the customer at the site and is owned by the customer. The password security meets Oracle standards. An infinite number of passwords is available for use over the life of the tape drive. If the admin password is forgotten, it can be reset. The first password is the default password sent with the tape drive.

## Enforce password management

Basic password management rules, such as password length, and complexity must be applied to the administrator password.

The password management rules require at least one of each of the following rules.

- Must be between 8 and 16 characters long
- Lower case (a-z)
- Upper case (A-Z)
- Decimal digit (0-9)
- Punctuation (.?;:"{}[]()!@#$%&, ...)

# 3

# Security Features

This section outlines the specific security mechanisms offered by the product.

Currently, all products in the T10000 family communicate on a secure channel to the Oracle Key Management System. Eventually, all products in the T10000 family will adhere to the SSH and SFTP security requirement. These should not be the only line of security to protect the Tape Drive. Ideally, the Tape Drives should be in a physically secured data center that also has a secured network that only allows access from the servers utilizing its functionality. These servers and applications running on them should also be secured. In addition, the customer has the option to elevate the security of the tape drive to yet another level. That level would be either to Encrypt their data and/or enable the FIPS (Federal Information Processing Standard) mode. The T10000 family of tape drives are FIPS compliant. See table below for supported levels. The link to the FIPS home page is:

http://www.itl.nist.gov/fipspubs/

| | |
|---|---|
| T10000A | FIPS 140-2 Level 1 |
| T10000B | FIPS 140-2 Level 2 |
| T10000C | FIPS 140-2 Level 1 |

# A

# Secure Deployment Checklist

The following security checklist includes guidelines that help secure the tape drive:

1. Enforce password management.
2. Enforce access controls.
3. Restrict network access.
   a. A firewall should be implemented.
   b. The firewall must not be compromised.
   c. System access should be monitored.
   d. Network IP addresses should be checked.
4. Contact Oracle Security Products if you come across vulnerabilities in Oracle tape drives.

# B

# References

You can access the VOP User Guide from:

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#vop