

**Oracle®**  
**StorageTek SL150 Modular Tape Library**  
**System**  
**Security Guide**

**E35113-01**

**2012**

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

Contents .....	3
Part 1: Overview .....	4
Product Overview .....	4
Security .....	4
General Security Principles.....	5
Keep Software Up To Date.....	5
Restrict Network Access.....	5
Keep Up To Date on Latest Security Information .....	5
Part 2: Secure Installation .....	6
Installation Overview .....	6
Understand Your Environment.....	6
Securing the Library .....	7
Installation Configuration .....	8
Part 3: Security Features .....	9
Part 4: Redeployment.....	10
Part 5: Appendices .....	11
Appendix A: Secure Deployment Checklist.....	11
References.....	12

## **Part 1: Overview**

This section gives an overview of Oracle's StorageTek SL150 Modular Tape Library System and explains the general principles of tape library security.

### **Product Overview**

StorageTek SL150 Modular Tape Library System is a 3U to 21U 19" rack mounted modular automated tape library by Oracle Corporation. It offers storage capacity of 30 to 300 LTO tape cartridges, from 1 to 20 LTO5 Half-Height Fibre or SAS tape drives, and a bridged drive Fibre or SAS port control path.

### **Security**

All tape library products are designed and documented for use within a controlled server environment with no general network or user access. This provides the best functionality and protection from compromise, both from the internet in general and from the internal entity operating the library.

## **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 a software level of:

Version 0.1.0.0.0.

### **Restrict Network Access**

Keep the library 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. Identifying the hosts allowed to attach to the library and blocking all other hosts is recommended where possible.

### **Keep Up To Date on Latest Security Information**

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

## **Part 2: Secure Installation**

### **Installation Overview**

This section outlines the planning process for a secure installation and describes several recommended deployment topologies for the systems.

#### **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 be provided.

From whom are the resources being protected?

The library must be protected from everyone on the Internet. But should the library 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 library. Understanding the security ramifications of each resource will help protect it properly.

## Securing the Library

This section describes how to secure the library.

By default, the library uses ports listed in Table 1 SL150 Network Ports. The firewall should be configured to allow traffic to use these ports and that any unused ports are blocked. Note that the SL150 initially only supports IPv4, but future enhancements may add IPv6 support.

Port	Type	Description
22	TCP	SSH CLI access – inbound stateful For development test and debug only, not available in the field
80	HTTP	WebLogic port for remote user interface
161	UDP	SNMP library agent requests - inbound stateful
162	UDP	SNMP library traps and inform notifications - outbound stateless for traps, outbound stateful for inform
67	DHCP	client - outbound
68	DHCP	client - inbound

Table 1: SL150 Network Ports

When configuring SNMP, using SNMPv3 is strongly recommended over SNMPv2c for its confidentiality, integrity and authentication capabilities.

## Installation Configuration

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

### **Assign the user (admin) password.**

At first power-on a setup wizard automatically runs on the local operator panel to obtain basic configuration information. This includes:

- Administrator account username and password
- Network configuration of Net1
- Setting date and time

The library is prevented from becoming operational until the setup wizard has been completed.

A login account is provided with the product shipment which the installer must enter as the first step in the setup wizard routine. The user must then enter a new password before the setup wizard will complete.

All other configuration is performed through the browser user interface (BUI).

### **Enforce password management.**

Basic password management rules, such as password length, history, and complexity must be applied to all passwords. SL150 passwords must be 8 characters or more and contain at least one numeric or special character. The default password must be changed during installation and may not be reused.



## **Part 3: Security Features**

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

The library provides an internal firewall to protect itself. This should not be the only line of security to protect the library. It is recommended the library is in a physically secured data center on a secured network only allowing access from servers utilizing its functionality. These servers and applications running on them should also be secured.

## Part 4: Redeployment

This section describes how the machine is returned to a factory default state.

In the event the customer needs to decommission a library, a procedure is provided which removes all customer configuration information and all log files, and returns the library to a factory default state. This procedure is invoked by placing the library in a “locate” mode and then simultaneously holding the front and rear locate buttons for greater than 10 seconds.

## Part 5: Appendices

### Appendix A: Secure Deployment Checklist

The following security checklist includes guidelines that help secure the library:

1. Enforce password management.
2. Enforce access controls.
3. Restrict network access.
  - i. A firewall should be implemented.
  - ii. The firewall must not be compromised.
  - iii. System access should be monitored.
  - iv. Network IP addresses should be checked.
4. Contact Oracle Security Products if you come across vulnerability in Oracle Tape Libraries.

# References

*SL 150 User Guide* located at:

[Tape libraries](#)