StorageTek SL4000 Modular Library System

Security Guide

E84232-02
February 2020

StorageTek SL4000 Modular Library System Security Guide,

E84232-02

Contents

Preface

1 Security on the SL4000

Preface

This guide provides security principles and guidelines for Oracle's StorageTek SL4000 modular tape library (SL4000).

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.

Related Documentation

Go to the Tape Storage section of the Oracle Help Center (https://docs.oracle.com/en/storage/tape-storage/index.html) for SL4000 documentation:

- *SL4000 Library Guide*
- *SL4000 SCSI Reference Guide*
- *SL4000 SCI Reference Guide*
- *SL4000 Security Guide*
- *SL4000 Safety and Compliance Guide*
- *SL4000 Licensing Information User Guide*

1 Security on the SL4000

To maximize security, you should follow general security principles, use key SL4000 security features, and follow best practices for the SL4000 tape library.

For an overview of the product, see the *SL4000 Library Guide*.

General Security Principles

Follow these fundamental principles to use the product securely.

Keep Software Up To Date

Keep all software versions and patches up to date. This document assumes a software level of version 1.0.

Restrict Network Access

Keep the library behind a data center firewall to restricted access to a known network route, which can be monitored and restricted if necessary. As an alternative, you can substitute a firewall router for multiple, independent firewalls. You should identify the hosts allowed to attach to the library and block all other hosts where possible.

Keep Up To Date on Latest Security Information

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

Network Access

Oracle designs and documents all tape library products for use within a controlled server environment with no general network or user access. Network access is required between the library and various other servers and workstations.

Network access is required for:

- Workstations used to access the library through the GUI or SCI interfaces

- Servers running applications that use the SCI interface, such as an ACSLS server or a custom application that uses SCI
- SMTP servers for sending e-mail notifications
- SNMP servers
- SDP2 server for "phone-home" (ASR) functionality
- Oracle Key Manager (OKM) clusters for delivering encryption keys to tape drives

User access to the library requires credentials (id and password) to be created on the library and to be used when connecting to the library.

Library Interface Credential Requirements

The library provides a browser-based GUI interface and a web services API (StorageTek Library Control Interface - SCI) for configuring, managing, and operating the library. Connecting with either interface requires valid user ID and password credentials.

When using the GUI, whether remotely with a browser or locally at the operator panel, you must provide a valid user ID and password to log in.

When using SCI, you must embed the user ID and password into the SOAP header of each SCI method call. The library uses the WS-Security SOAP extension as defined by OASIS WS-SecurityPolicy 1.2 (July 2007). Because the credentials in the header are in plain text, SCI must use an HTTPS connection. The exact details of how to include the SOAP headers depends on the language used to invoke the web services API.

Users and Roles

There are two categories of users – customer (with four roles: Viewer, Operator, User, and Administrator) and service (with three roles: Service, Advanced Service, and Escalation). A user's role determines their access to GUI functions and SCI methods.

- See the “User Roles" section of the *SL4000 Library Guide* for role descriptions and authorized GUI functions.

Creating Customer Users

The administrator can use the GUI to create customer users by defining the user ID, password, and role (see the “Add, Modify, or Delete a User" section in the *SL4000 Library Guide*). Passwords must be at least eight characters long and include a mix of letters (uppercase or lowercase) and numbers.

Creating Service Users

Service users are either automatically generated by the library following the detection of a fault or manually created by the administrator. Service users have a specified role, but a randomly generated user ID and encrypted password (known as a key file). Oracle Services can decrypt the key file to provide the credentials to a field engineer. Service users expire 72 hours after creation and cannot be extended.

When the library detects a fault, it automatically creates a user with the "Service" role and generates an encrypted support bundle (which contains the service key file). You must manually transmit the support bundles to Oracle Service, unless you have configured the library to perform Automated Service Requests (ASR). If the fault requires more than 72 hours to resolve or requires a higher-level service role, the administrator may need to create an additional service user ID through the GUI (see the “Add a Service User" in the *SL4000 Library Guide*).

Certificates for HTTPS Interfaces

To ensure the security of connections over HTTPS, a certificate is required on the library.

The library supports three certificate types:

- Default certificate (weak encryption, not recommended for use beyond installation)
- Self-signed certificate (strong encryption, but requires a security exception in the browser)
- Third-party signed certificate (strong encryption, guaranteed security, automatically accepted by most browsers)

During initial installation, the library uses the default certificate. You should replace it by generating a new self-signed certificate (see "Generate a Self-Signed Certificate" in the *SL4000 Library Guide*). Using a self-signed certificate is secure, but will cause browsers to generate a warning when connecting to the library. To avoid this warning, you must configure a security exception in the browser or install a third-party signed certificate.

After generating a self-signed certificate, you may install a third-party signed certificate which offers the strongest encryption and security, and eliminates the need for a browser security exception. Creating a properly signed certificate is a two step process. First, download the certificate signing request (CSR) from the library and submit the CSR to a third-party certifying authority (CA). Then, once the CA creates the signed certificate, upload it to the library along with a copy of the CA's certificate (see "Install a Third-Party-Signed Certificate" in the *SL4000 Library Guide*). Provided the certificate is signed by a well known CA, the browser will connect over HTTPS without warnings.

Library Network Interfaces

The library has four external network interfaces located in the Base Module's card cage on the Library Controller and Root Switch Cards.

- Customer ports — Used to connect the library into the customer's network. Used for library management functions (configuration, code upgrades, monitoring, and so on). Used by applications that use the web services interface (SCI).
- Service port — May be used to connect to a "phone home server" (specifically Automated Service Requests (ASR) using SDP2). If connected to SDP2, the port will be connected continuously. Service engineers can also use this port while servicing the library.
- OKM port — Used to connect the library to an Oracle Key Management (OKM) cluster. However, you may connect to an OKM cluster using the Service or Customer interface.
- Inter-library ports — These ports are disabled and not used in a SL4000 library.

For a diagram of the physical locations of the ports, see "Base Module Card Cage" in the *SL4000 Library Guide*.

Default Port Numbers

By default, the library uses the port numbers listed in the table below. If using a firewall, configure it to allow traffic to use these ports.

Enable the ports listed below on each of the network interfaces that are in use (except the OKM ports — you only need to enable the OKM ports on the network interface used to connect to the OKM cluster).

Port	IP	Protocol	Description	Direction
22	TCP	SSH	SSH access to Linux running on library. Only enabled for 72 hours after an "Escalation" role service user is created.	To library
25	TCP	SMTP	Connection to external SMTP (Simple Mail Transfer Protocol) server. Required if you have configured any e-mail destinations.	From library
53	TCP & UDP	DNS	DNS (domain name server) lookup.	From library
80	TCP	HTTP	Default port for browser access.	To library
161	UDP	SNMP	Inbound GET requests through SNMP.	To library
162	UDP	SNMP	Outbound SNMP TRAPs.	From library
123	TCP	NTP	Connection from library to an external NTP server.	From library
443	TCP	HTTPS	Default port for browser and web services interfaces.	To library
7104	TCP	HTTP	Alternate port for browser access.	To library
7102	TCP	HTTPS	Alternate port for browser and web services interfaces.	To library
7104	TCP	HTTP	Browser GUI based access to WebLogic console running on the library. Only accessible by an "Escalation" user.	To library
7105	TCP	HTTPS	Browser GUI based access to WebLogic console running on the library. Only accessible by an "Escalation" user.	To library
Externally Defined	TCP	HTTP & HTTPS	Servers that are configured to receive outbound SCI calls will listen for SCI calls on ports of their choice. Open these port number in any firewalls and provided the port numbers configuring the destination on the library.	From library
Externally Defined	TCP	OKM	If the library is configured to retrieve tape drive encryption keys from a OKM cluster, open the ports used for OKM (see the OKM documentation).	From library

Browser and Web Services Interfaces

The GUI can use both HTTP and HTTPS. The SCI interface uses only HTTPS to secure for the credentials passed in each request. By default, these two protocols are on their standard port number of 80 for HTTP and 443 for HTTPS. You can modify these ports in the GUI (see "Configure the Library with the Configuration Wizard" in the *SL4000 Library Guide*).

Service Access

Under normal library operations only customer-created users may log in to the library However, the administrator can enable service access when necessary (see Creating Service Users). Creating a service user with an Escalation role enables access to the library that is not normally allowed. Specifically, an Escalation user can log in to Linux on the library using SSH on port 22 and can access the WebLogic console function using port 7104 for HTTP or 7105 for HTTPS. Service users expire 72 hours after creation. The library disables port 22 if there are no enabled service users. The library always enables ports 7104 and 7105, but unless an Escalation user exists, there are no valid users that can log in to the WebLogic console.

SNMP

The library supports SNMP v3 protocol. The library uses ports 161 (inbound) and 162 (outbound) for SNMP GET commands and SNMP traps respectively.

E-mail

The library can send e-mail messages when certain events occur (see "Configuring Notifications" in the *SL4000 Library Guide*). If you configure e-mail destinations, you must also configure an SMTP server and open port 25.

DNS

DNS configuration is optional. You only need to configure DNS if destinations (SNMP, E-mail, Outbound SCI) use host names. You can add up to three DNS servers (see "Configure the Library with the Configuration Wizard" in the *SL4000 Library Guide*). DNS uses port 53.

NTP

The library can use an external NTP server to control the library clock. If using an external NTP server, you must open port 123.

Oracle Key Manager (OKM)

You can connect an OKM cluster to the library's customer port, service port, or OKM port. The location of the OKM appliance within your network determines which port you should use. You select the port during network configuration of the library (see "Configure the Library with the Configuration Wizard" in the *SL4000 Library Guide*). Unlike older tape libraries, the SL4000 only requires a single connection to OKM, rather than individual connections to each encrypted tape drive. You must open the ports used by OKM on the selected connection. See the OKM documentation for details on which port numbers to use.

Handing-Off the Library to the Customer

An Oracle installation engineer will install and test the SL4000 library using a pre-defined user ID ("installer") which initially uses with a well-known password. The first step the installer performs is to change this password.

After testing the SL4000, the installation engineer begins the hand-off process to transfer the library to the customer. The hand-off involves creating an Administrator user and finalizing the HTTPS certificate. The installation engineer initiates the hand-off, but the library administrator must complete the process.

Creating the Administrator User

In the first step of the hand-off, the administrator enters a user ID and password to create the Administrator account. After completing the hand-off, the library will remove the Installer user and the newly created Administrator user will be the ONLY account that can log in to the library.

Configuring the HTTPS Certificate

In the second step of the hand-off, the administrator configures the certificate for HTTPS. There are two options:

1. Continue to use the default certificate (not recommended)
2. Generate a new self-signed certificate.

If you do not generate a self-signed certificate, you can still access the library using HTTPS, but it will use the weakest form of encryption. If you generate a self-signed certificate, the library begins using it immediately. For best security, you should replace the self-signed certificate with a third-party signed certificate (see "Install a Third-Party Signed Certificate" in the *SL4000 Library Guide*).

Redeployment

If you need to decommission the library, an Administrator or Service user can reset the library to factory defaults through the GUI.

Resetting removes all configuration information. You CANNOT undo this action. Redeploying the library will require Oracle Services to re-perform the installation and customer hand-off.

Secure Deployment Checklist

Use this checklist to help secure the library.

- Enforce password management
- Enforce access controls
- Restrict network access
  - Implement a firewall
  - The firewall must no be compromised
  - Monitor system access

- Check network IP addresses
- Contact Oracle Security Products if you encounter any vulnerability in Oracle tape libraries