StorageTek Tape Analytics

Security Guide

Release 2.4

F33185-01

July 2021

StorageTek Tape Analytics Security Guide, Release 2.4

F33185-01

Contents

Preface

This document describes the security features of Oracle's StorageTek Tape Analytics (STA) version 2.4.x.

Audience

This guide is intended for anyone involved with the secure installation and configuration of STA.

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

View additional STA documentation at: `https://docs.oracle.com/en/storage/storage-software/storagetek-tape-analytics/`

1

Secure Installation and Configuration

Plan for a secure installation and follow recommended deployment guidelines when applicable.

- General Aspects of Security
- General Security Principles
- Understand Your Environment
- Installing StorageTek Tape Analytics (STA)
- Post Installation Configuration
- Certificate for HTTPS Communication
- Users and Credentials
- Secure Deployment Checklist

General Aspects of Security

The main aspects to STA security are: physical, network, user access, and server access.

Physical

You must install STA on a standalone server. Your company's policy should dictate who has physical access to the server. For maximum security, the server should be in a physically secured data center, which also has a secured network that allows access only to authorized users.

Network

It is required that STA be added or configured to a customer internal firewall-protected network. This network needs SSH and SNMPv3 access to libraries for which data will be accessed.

To use the user interface, you need HTTPS access.

To enable optional log bundle forwarding to StorageTek Service Delivery Platform (SDP), a connection to the SDP host is also required within the customer internal firewall-protected network.

User Access

The STA application access is controlled by user name and password authentication. User names and passwords are set up during initial installation by the customer. Passwords must meet Oracle standard requirements.

Server Access

STA requires an OS level Oracle user for installation and run-time access.

You should limit the access to the server, especially super users (root), which could affect the STA application, functionality, and services.

General Security Principles

Follow fundamental principles to securely use the STA application.

Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date.

> **Note:**
>
> The libraries and drives must also meet minimum firmware version levels that are connected to the STA application. These firmware levels are specified in the Requirements for STA section of the *Installation and Configuration Guide*.

To enable the best security available, Oracle recommends keeping the OS and all application components (like Weblogic, ADF, Java, and so on) up to date with the latest security patches. Oracle periodically provides security patches for components (like Weblogic, ADF, MySQL and Java) through the Oracle CPU (Critical Patch Update) advisories and other communications.

Because OS security patches are independent of the STA application, Oracle cannot guarantee that all patches will operate correctly with STA—especially patches released after an STA release. Determine the acceptable OS security patch level for your environment. Because of component patch and application interdependencies, Oracle cannot guarantee that all component patches will operate correctly with the STA application. Determine which component patches are needed for your environment and what affects it may have on the STA application.

Newer STA versions and STA specific patches may also be available. Check with Oracle service on the availability of a newer version of STA or an STA specific patch. Newer STA versions will contain more up to date security patches.

> **WARNING:**
>
> Oracle strongly recommends using only trusted sites. Validate the source of all software downloads and patches to ensure that they do not contain any security vulnerabilities like malware, viruses, worms, and so on.

Restrict Network Access

Oracle recommends that you keep the STA host server behind a data center firewall. The firewall restricts access to these systems 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. STA is not designed to be directly accessible from a public network.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. For every STA release review the document for revisions. Specific security concerns may be addressed in release notes as well.

Understand Your Environment

Address key questions about your environment to better understand your security needs.

Which resources need to be protected?

For STA, the host server and the associated network must be protected from unauthorized access.

From whom are the resources being protected?

STA must be protected from everyone on the Internet, external users, and unauthorized internal users. You should ensure that you have intrusion protection and monitoring software.

What will happen if the protection on strategic resources fail?

As STA is a device monitoring and usage application, unauthorized access to STA will only affect STA. The monitored devices and associated data will not be affected.

Installing StorageTek Tape Analytics (STA)

Only install STA on a system that is within the same protected (firewalled) network infrastructure as the monitored libraries. You should enforce customer access controls on the systems where STA is installed to restrict access to the application.

Refer to the *Installation and Configuration Guide* for installation instructions.

The STA installer may modify permissions on some files and directories to allow the STA application running as Oracle user access to certain files. For example: /etc/.java.

Firewall Port Assignment

The firewall must allow communication on the ports used by the STA application. For a list of ports, see the following:

- Unconfigurable Ports
- Configurable Ports
- Ports for Communications with SDP (optional)

Firewall Configuration

Firewall configuration is dependent on the OS version. Review the configuration of the iptables and troubleshooting sections as needed.

- Enable the Linux Firewall iptables in the *Installation and Configuration Guide*
- Troubleshooting appendix in the *Administration Guide*

Unconfigurable Ports

Some port values are fixed and cannot be changed during STA installation or after.

The firewall must allow communication between the STA server and the backup server (for SSH), and between the STA server and the monitored libraries (for SNMP and SNMPTRAP).

Port	Protocol	Description
22	SSH	Secure Shell. STA database backup; library log-in.
161	SNMP	Simple Network Management Protocol (SNMP). For transmittal of SNMP requests.
162	SNMPTRAP	For reception of SNMP notifications (traps). Traps are forwarded to configurable unprivileged internal port (default is 7027).

Configurable Ports

Configurable ports are initially defined during STA installation, but can be changed using the Port Change Utility. The utility automatically verifies that the new ports are not already in use on the network and updates all appropriate processes on the STA server to use the new ports.

> **Note:**
>
> See your network administrator for assistance with port number assignments. Although it is permissible to have two different processes assigned to the same port number if they use different protocols, this practice is not recommended.

External Ports

These ports are the configurable equivalent of standard ports 80 and 8080 (HTTP) and 443 (HTTPS), and they must be unique from other HTTP and HTTPS ports on the network. The firewall must allow communication between the STA server and the client running the STA GUI.

Default Port	Protocol	Description
7019	HTTP	Access to the WebLogic Administration console, unsecure
7020	HTTPS	Access to the WebLogic Administration console, secure
7021	HTTP	staUi managed server. Access to the STA GUI, unsecure.
7022	HTTPS	staUi managed server. Access to the STA GUI, secure.

Internal Ports

Default Port	Protocol	Description
7023	HTTP	staEngine managed server. Basic STA internals, unsecure.
7024	HTTPS	staEngine managed server. Basic STA internals, secure.
7025	HTTP	staAdapter managed server. SNMP communication, unsecure.
7026	HTTPS	staAdapter managed server. SNMP communication, secure.
7027	SNMPTRAP	Internal unprivileged port for SNMP traps forwarded from external privileged port 162.

Ports for Communications with SDP (optional)

STA 2.4.x supports optional automatic creation of service log bundles and forwarding of the bundles to StorageTek Service Delivery Platform (SDP). Communication with SDP requires specific port configuration.

See the following documents for details about these optional features:

- *STA User's Guide* for information on configuring and using these features in STA.
- *StorageTek Service Delivery Platform User's Guide* for information on configuring and using these features on the SDP host.

The table below summarizes the ports on the STA server that are used for communications with the SDP host.

Table 1-1 Ports for Communications With StorageTek SDP

Port	Protocol	Description/Purpose
7023 (default)	HTTP	Inbound communications from the SDP host to STA. Messages from SDP come in on the unsecure port assigned to the staEngine managed server. See Configurable Ports.
7024 (default)	HTTPS	Inbound communications from the SDP host to STA. Messages from SDP come in on the secure port assigned to the staEngine managed server. See Configurable Ports.
15000 (default)	Java RMI	Outbound communications from STA to the SDP host. You identify this port when configuring the SDP host in STA which tells STA the destination port on the SDP platform. The port must match the port that the SDP machine has open for client communications. See Define the SDP Host to STA in the *STA User's Guide*. The same port number must be configured on the SDP host to receive messages from STA. See the *StorageTek Service Delivery Platform User's Guide* for instructions.

Post Installation Configuration

There are no post-installation configuration security changes. The installation process has you configure administration accounts, passwords, and ports. If necessary after installation, you can use the Password Change Utility to update passwords or the Port Change Utility to alter ports.

User (admin) Password Configuration

The installation process has you configure the administration account and password. You can use the Password Change Utility to update administration and database accounts after the installation.

See Change a Password with the Utility in the *Administration Guide* for more information.

Enforce Password Management

STA enforces minimum requirements on all passwords. You should always apply password management rules such as password length, history, and complexity to the all passwords. Oracle recommends periodically changing passwords to maximize security.

Port Assignment

The installation process has you configure port numbers. You can use the Port Change Utility to update the configurable ports after the installation.

See Change Ports Using the Utility in the *Administration Guide* for more information.

Certificate for HTTPS Communication

STA uses a digital certificate for HTTPS communication. Both the GUI and SCI use the same certificate.

SCI/GUI Certificate

Weblogic uses HTTPS for communication between the browser and server, as well as the server and SL4000 library. This requires a security certificate. You can use the auto-generated, self-signed certificate or provide a third-party signed certificate.

Auto-Generated, Self-Signed Certificate

Weblogic ships with a default 'demo' certificate which provides minimal encryption security. The STA installation automatically overwrites this certificate with an auto-generated certificate which has a 2048 bit key. The certificate is valid for 1824 days. Self-signed certificates cause most browsers to present a security exception, which the user will have to accept when connecting to the user interface.

Third-Party Signed Certificate

To eliminate the browser security exception, you can use a third-party signed certificate. The procedures for generating a third-party certificate for WebLogic can be found here: http://docs.oracle.com/cd/E13222_01/wls/docs92/secmanage/identity_trust.html

To update the certificate within WebLogic, see "Reconfigure WebLogic to Use a Different Security Certificate" in the *STA Installation and Configuration Guide*.

Users and Credentials

A user's role determines their access to STA GUI functions. Communication between STA and the tape libraries requires several different sets of credentials.

STA User Roles

Each STA user has an assigned role (Viewer, Operator, or Administrator), which determines what the user can access.

See User Roles and Privileges for more information.

SNMPv3 Credentials (SL150, SL500, SL3000, SL8500)

Communication between the STA server and SNMP library interfaces (SL150, SL500, SL300, SL8500) requires SNMPv3 user, authentication, and privacy credentials. You must maintain these credentials on the library and on STA.

See Configure SNMP Client Settings for STA in the *STA Installation and Configuration Guide* for details on configuring the credentials.

SCI Credentials (SL4000)

HTTPS communication using standard TLS protocol from STA to an SL4000 library requires SCI credentials. Before connecting the library to STA, you will need to define credentials with the “User” role on the library side. Oracle recommends using different usernames and passwords for each SL4000 library connected to STA. A secure wallet within STA stores the credentials for each SL4000 library connected to it.

See the "Add, Modify, or Delete a User" section in the *SL4000 Library Guide* to create a user on the library.

See Add the SL4000 as a Monitored Library in the *STA Installation and Configuration Guide* to configure the connection.

OSCI Credentials (SL4000)

HTTPS communication using standard TLS protocol from an SL4000 library to STA requires OSCI credentials. Within STA, you will need to define credentials with the "Operator" role. The SL4000 then stores these credentials within a secure wallet on the library.

See Add, Modify, or Delete a User in the *STA User's Guide* to create a user.

See Add the SL4000 as a Monitored Library in the *STA Installation and Configuration Guide* to configure the connection.

SMTP Email Server

You can configure the emails sent from STA to use a secure connection protocol (either standard TLS or SSL) and provide credential information if the SMTP server requires authentication.

See Define the SMTP Email Server in the *STA User's Guide*.

External Authentication Providers

You can configure Oracle's WebLogic Server to use one or more external authentication providers to authenticate users for STA.

See Configure External Authentication Providers in the *STA Installation and Configuration Guide*.

Secure Deployment Checklist

Complete the deployment checklist to help secure your system.

1. Enforce password management.
2. Enforce access controls.
3. Restrict physical access to the server.
4. Restrict network access.
   a. Implement a firewall.
   b. Monitor system access.
   c. Check network IP addresses.
5. Install intrusion monitoring software.
6. Contact your Oracle services, tape library engineering, or account representative if you come across vulnerabilities in Oracle hardware and applications.