StorageTek Tape Analytics

Installation and Configuration Guide

Version 2.4
F33183-04
January 2022

ORACLE

StorageTek Tape Analytics Installation and Configuration Guide, Version 2.4

F33183-04

Contents

3 Install and Configure Linux on the STA Server

4 Install STA

5 Configure Library Features for STA

6 Configure the Library Connection (SNMP or SCI)

7 Upgrade to STA 2.4.0

B Silent-mode Installer

C Record Installation and Upgrade Information

D Configure Security Certificates

E Configure External Authentication Providers

F Troubleshoot Issues

Preface

This document provides installation requirements and planning information Oracle's StorageTek Tape Analytics (STA) version 2.3.1. It describes how to install Linux, install STA, and configure STA to begin monitoring tape libraries. It also describes how to upgrade and uninstall 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/

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers and partners we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

Requirements for STA

The installation environment must meet minimum requirements to use STA 2.4.x.

Devices Supported by STA

STA supports specific models of tape libraries, drives, and media. Before installing STA, verify that the models within your library system are supported.

In general, the newer the model and the more up-to-date the firmware, the richer the data that STA will receive, allowing STA to perform a more in-depth the analysis. For best results, update your drive and library firmware to the most current versions.

See Library Requirements and Tape Drive Requirements for minimum firmware levels and other requirements.

Tape Libraries

- SL8500
- SL4000
- SL3000
- SL500
- SL150

Drive and Media Types

- StorageTek T10000A, B, C, and D drives (with T10000 T1 and T2 media)
- StorageTek 9840C and 9840D
- HP LTO generations 3, 4, 5, and 6
- IBM LTO generations 3, 4, 5, 6, 7, 8 and 9
- LTO M8 media is only supported by STA 2.3.1 and above

> **Note:**
>
> LTO-8 and above can read and write one generation back. LTO-7 and below can read two generations back and write one generation back. For best capacity and performance, always use cartridges of the same generation as your drives.

Automation Drive Interface (ADI) Protocol

For LTO drives, you must enable the ADI protocol on both the drives and the library for STA to receive rich data about these drives. LTO-2 and SDLT drives do not support ADI, and therefore STA receives only minimal data about them. See LTO Drive Requirements.

Library Requirements

Verify the tape libraries within your system meet minimum requirements for STA.

For the best functionality, upgrade to the recommended or latest available library firmware. Firmware versions are subject to change. See Verify the Library Firmware Version to check the current library firmware version. To upgrade your firmware, open a Service Request (SR) with your Oracle support representative.

Table 1-1 Library Firmware Requirements

Feature	SL150	SL500	SL3000	SL4000	SL8500
Recommended for full STA features in this release. Newer firmware may be available.	3.87	FRS 1501	FRS 4.58	1.1.1	FRS 8.75
Minimum for STA compatibility. Some STA features may not function with older firmware.	1.82	FRS 1485	FRS 3.61	1.1.1	FRS 8.01
Minimum for LTO media validation	3.87	Not supported	FRS 4.58 SLC 6.71	Not Supported	FRS_8.75 SLC 6.71
Minimum for T10000 media validation	Not supported	Not supported	FRS_4.30 SLC 6.50	Not Supported	FRS_8.31 SLC 6.25
Minimum for IBM LTO-9 drives	3.87	Not supported	FRS_4.58	1.1.1	FRS_8.75
Minimum for IBM LTO-8 drives, with or without encryption	3.20	Not supported	FRS_4.50	1.1.1	FRS_8.60
Minimum for IBM LTO-7 drives, with or without encryption	2.60	Not supported	FRS 4.40	1.1.1	FRS 8.51
Minimum for IBM LTO-6 drives, with or without encryption	2.25	Not supported	FRS 4.31	1.1.1	FRS 8.36
Minimum for IBM LTO-5 drives, with or without encryption	Not supported	FRS 1493	FRS 4.31	1.1.1	FRS 8.36
Minimum for IBM LTO-4 drives with encryption	Not supported	FRS 1493	FRS 4.31	Not supported	FRS 8.36

Table 1-1 (Cont.) Library Firmware Requirements

Feature	SL150	SL500	SL3000	SL4000	SL8500
Minimum for HP LTO-6 drives	1.82	FRS 1485	FRS 3.61	1.1.1	FRS 8.01
Minimum for HP LTO-5 drives	1.82	FRS 1485	FRS 3.61	1.1.1	FRS 8.01
Minimum for all other drives (such as T10000).	Not supported	FRS 1485	FRS 3.61	1.1.1	FRS 8.01

Table 1-2 Library Hardware Requirements

Library	Component	Requirements
SL3000 SL8500	HBT card	**High-memory drive controller (HBT) card**: Required for media validation support and reporting of richer drive data. Libraries with LTO drives must have a high-memory HBT card to enable ADI. See the Verify the HBT Drive Controller Card Version (SL3000 and SL8500 only) to determine the memory level of your HBT card. **Note**: All SL3000 libraries ship with the high-memory card. Since 2006, all SL8500 libraries ship with the high-memory card.
SL8500	Complex	All SL8500 libraries in a single complex must be monitored by a single instance of the STA application.
All	Ethernet connection	**Separate connection from STA to each library**: Each library must have an assigned IP address and be reachable by the STA server. **Note**: Each library in an SL8500 complex has its own SNMP agent. Therefore, STA must be able to connect to each library separately.

Tape Drive Requirements

Verify the drives within your library system meet minimum requirements for STA.

- StorageTek Drive Requirements
- LTO Drive Requirements

StorageTek Drive Requirements

To maximize the quality of data received from T10000 and T9840 drives, you should use the highest TTI level and firmware supported by the drive model.

Firmware versions are subject to change. The media validation (MV) Complete Verify Plus test is not supported in FICON environments (applies to TTI 5.40 and TTI 5.5.0 only). To upgrade your firmware, open a Service Request (SR) with your Oracle support representative.

Table 1-3 Minimum StorageTek Tape Drive Firmware Requirements

Drive	Recommended for STA	TTI 5.10	TTI 5.20	TTI 5.30	TTI 5.40	MV Support TTI 5.40	MV Support TTI 5.50	TTI 5.60
T10000D	4.18.103	Not Supported	Not Supported	Not Supported	4.07.104 (FC) 4.07.106 (FICON)	4.07.107	4.08.107	4.14.106
T10000C	3.69.103	Not Supported	1.51.320	1.53.316	1.57.308	1.59.302	3.62.111	Not Supported
T10000B	1.52.206	1.44.208	1.46.209	1.52.203	Not Supported	Not Supported	Not Supported	Not Supported
T10000A	1.52.106	1.44.108	1.46.109	1.52.103	Not Supported	Not Supported	Not Supported	Not Supported
9840D	1.47.702	1.44.710	1.47.702	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
9840C	1.47.502	1.44.510	1.47.502	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported

LTO Drive Requirements

To maximize the quality of data received from LTO drives, enable ADI and use the highest firmware level supported by the drive model.

ADI Requirements

LTO drives that support the Automation/Drive Interface (ADI) can provide rich data (for example drive performance and utilization). For a library to send rich LTO drive data to STA, ADI must be enabled on both the library and the LTO drives. If ADI is not enabled on both, the library will only send basic data about the LTO drives.

For SL3000 and SL8500 libraries, you can enable ADI only if the library has a high-memory drive controller (HBT) card. See Library Requirements. Enabling ADI requires a reboot of the library. Therefore, you should enable it in advance if you are planning to install LTO drives. See Enable ADI on the Library (SL500, SL3000, SL8500).

Media Requirements

LTO M8 media is only supported in STA 2.3.1 and above.

Firmware Requirements

Firmware versions are subject to change. To upgrade your drive firmware, open a Service Request (SR) with your Oracle support representative.

Table 1-4 LTO Drive Firmware Requirements

Drive Type	Recommended for STA	Minimum
IBM LTO-9 Full-height FC	N7N0	N7N0
IBM LTO-9 Half-height FC/SAS	N9B1	N9B1

Table 1-4 (Cont.) LTO Drive Firmware Requirements

Drive Type	Recommended for STA	Minimum
IBM LTO-8 Full-height FC	KAH0	H9E2
IBM LTO-8 Half-height FC/SAS	KAH1	H9E3
IBM LTO-7 Full-height FC	KAH0	FA14
IBM LTO-7 Half-height FC/SAS	KAH1	G341
IBM LTO-6 Full-height FC	KAJ0	E4J0
IBM LTO-6 Half-height FC/SAS	KAJ1	G9P3
IBM LTO-5 Full-height FC	G360	E4J0
IBM LTO-4 Full-height FC	C7QH	C7QH
HP LTO-6 Full-height FC	J5ES	J2DS
HP LTO-6 Half-height FC	25FS	22GS
HP LTO-6 Half-height SAS	35FS	32DS
HP LTO-5 Full-height FC	I6PS	I3CS
HP LTO-5 Full-height SAS	X6JS	X3AS
HP LTO-5 Half-height FC	Y6KS	Y5BS
HP LTO-5 Half-height SAS	Z6HS	Z55S
HP LTO-4 Full-height LVD SCSI	B63S	B57S
HP LTO-4 Full-height FC 4Gb	H67S	H58S

Refer to the Oracle Key Manager (OKM) documentation for encryption card requirements.

Server Requirements

Verify that the server you plan to use for STA meets minimum requirements.

To ensure optimal performance and functionality of the STA application, you must install STA on a dedicated server. Oracle can only provide support if the server is dedicated to STA and not running any other application.

- Server Sizing and Considerations for Larger Installations
- Server Hardware Requirements
- Server Operating System Requirements
- Server Network Requirements and Recommendations

Server Sizing and Considerations for Larger Installations

Larger library environments are more demanding on the STA server. The minimum server size required depends on the number of libraries, slots, drives, media, and exchanges per hour.

Before you install or upgrade to the latest version of STA, contact your Oracle sales representative for assistance with sizing your STA server. The sales representative can use

the STA Server Sizing Tool to provide you with sizing recommendations to meet your site's current needs and expected growth.

Memory swap size must be 50 to 100 percent of RAM size. See Review the STA File System Layout.

If you have significant exchanges per hour (greater than 300) with multiple libraries attached to a single STA server and a long history with STA, you should carefully consider the size of the following key areas:

- Operating system and main application area — Oracle recommends this to be on its own appropriately sized HDD. The Oracle storage home location (for example, `/Oracle`) needs to be at least 100 GB, but you should allocate 200 GB if `/tmp` is in the root partition. Allocate another 200 GB if `/var/log/tbi` is also in the root partition.
- STA database data (for example, `/dbdata`) — Oracle recommends this to be on its own appropriately sized HDD. Guidance is from 250 GB up to 500 GB.
- STA database backups (for example, `/dbbackup`) — Oracle recommends this to be on its own appropriately sized HDD. Guidance is from 500 GB up to 2 TB.

You may also want to consider using SSDs.

Server Hardware Requirements

The server hardware must meet minimum requirements to run STA.

To accommodate future STA upgrades or library changes, select a server that has expandable disk bays, CPU cores, and RAM slots. Contact your Oracle sales representative for assistance with sizing your STA server.

Table 1-5 Server Hardware Requirements

Hardware	Configuration
Processor	Intel Xeon Series or equal AMD CPU
CPU cores	Minimum: 6 Recommended: 12 to 32, or capability to expand to this configuration
Memory	Minimum: 16 GB RAM Recommended: 32 GB to 128 GB RAM
Operating system disk	Dual HDD drives: • 600 GB each (single library, typical) • 1 TB each (multiple libraries, typical) **Note**: As the number of data exchanges increases, so does the size of the database.
Database data and local backup disks	Minimum: 100 GB each Recommended: 250 GB to 2 TB each
Connection	Gigabit Ethernet
Platform	All disk storage residing on a single platform See the Review the STA File System Layout for the recommended file system layout and allocations.

Server Operating System Requirements

STA 2.4.0 is supported on Oracle Linux 7.8 and 7.9.

STA does not support SELinux. You must disable SELinux before installing STA.

Table 1-6 Operating System Requirements

Operating System	Supported Version
Oracle Linux, 64-bit (Oracle kernel)	7.8, 7.9

Server Network Requirements and Recommendations

The network must meet minimum requirements to support STA.

- The STA server must have a static IP address.
- Oracle recommends that you place the STA server on the same subnet as the libraries to improve SNMP UDP reliability.
- If you configure STA to support dual TCP/IP using two distinct subnets, configure the network to allow the delivery of SNMP packets on either subnet between the library and STA. Consult your network administrator and your Oracle support representative for more information.

User Interface Requirements

The browser must meet minimum requirements to run the STA browser interface.

Table 1-7 User Interface Requirements

Item	Minimum Requirements
Browser	Some browsers may not render the STA interface properly. If you encounter issues, make sure your browser is up to date, or try a different browser. Recommended browsers: • Mozilla Firefox • Google Chrome • Microsoft Edge
Browser Settings, Plugins, and Add-ons	Enable JavaScript. Run all browsers in Native Mode. Disable or remove third-party add-ons.
RTL Language Support	Support for right-to-left (RTL) languages is available only with Internet Explorer 8.0 or 9.0.
Screen Reader Assistive Technology	The latest version of JAWS is recommended. See the *STA User's Guide* for accessibility information.

Media Validation Requirements

The library, drives, media, and STA must meet minimum requirements to use media validation.

STA Requirements

- STA 2.3.0 or above (for SL8500 and SL3000)
- STA 2.4.0 or above (for SL150)
- Connect to libraries using SNMP v3 protocol for SL150, SL3000, and SL8500.
- Use only one instance of STA to perform media validation activities. The use of multiple instances on the same library is not supported.

Library Requirements

- Compatible library firmware. See Library Requirements.
- Dedicated pool of media validation drives defined using the library interface.
- Valid cleaning cartridges for the media validation drives. The cartridges must be within the system cells.
- High-memory HBT card (for SL3000 and SL8500).

Drive Requirements

- T10000C or D drives using compatible firmware (for SL3000 or SL8500). See StorageTek Drive Requirements.
- IBM LTO 6+ drives (SL150), IBM LTO 6+ drives in ADI mode (for SL8500)
- Drives used to validate encrypted media must be enabled for encryption and connected to Oracle Key Manager (OKM).

Media Requirements

- A compatible drive must be within the media validation pool.
- Media validation is not supported for media formatted with StorageTek Automatically Linked Partitioning (ALP) done with Oracle's StorageTek Virtual Storage Manager (VSM).

SDP Interface Requirements

STA and StorageTek Service Delivery Platform (SDP) must meet minimum requirements to enable forwarding of automatic support bundles.

Depending on your site's configuration of SDP and Oracle Auto Service Request (ASR), SDP may automatically create Service Requests and forward the STA log bundles to My Oracle Support (MOS). SDP and ASR services are separate from STA.

STA supports automatic bundle forwarding to only one SDP host. However, you can connect any number of STA servers to the SDP host.

STA Requirements

- STA 2.3.0 or above.
- Internet connection to the SDP host.
- IP address and host name of the SDP host must be defined on the network.
- Ports must be assigned on the STA server for communications between STA and the SDP host.

SDP Requirements

See the *SDP2 User's Guide* for complete requirements and configuration instructions.

- Minimum version 2.5.2.
- SDP host must be registered with and connect to My Oracle Support (MOS).

Where to Find SDP Documentation

SDP documentation is on My Oracle Support: `https://support.oracle.com`

Sign in to MOS and then search for **Doc ID 1926810.2** to locate the *Information Center: VOP-SDP2 Overview Advisor*.

IBM RACF Mainframe Requirements

The system must meet minimum requirements to configure STA for RACF authentication.

See the Configure IBM RACF Authentication Providers for instructions on configuring STA for RACF. You must install two separate packages to configure RACF for STA:

- RACF service for STA, which is part of the SMC component of ELS 7.0 and 7.1. You must install the PTF to support this RACF service on the mainframe.
- WebLogic RACF Security Service Provider (or RACF SSP) that must be installed into WebLogic.

Table 1-8 IBM RACF Software Requirements

Software/Firmware	Version
ELS PTF versions for STA/RACF **Note**: STA/RACF is *not* supported in HSC 6.2.	ELS 7.0 - L1H16DH (MVS) ELS 7.1 - L1H16DI (MVS) ELS 7.2 - in the base code (MVS)
IBM PTF versions (for APAR PK69048) for AT-TLS encryption to NCS/ELS HTTP server connection	Best performance: z/OS 1.10 - Release 1A0: UK39417 available 08/10/07 Minimum for the Communication Server: z/OS 1.9 - Release 190: UK39419 available 08/10/07

2
Pre-installation Planning

Before installing STA, review best practices and make sure you understand the installation process.

- STA Deployment Process Overview
- Best Practices for STA Deployment
- Prepare Service Requests for the Libraries and Drives

STA Deployment Process Overview

To install and configure STA for the first time, you must perform activities in the order listed. You can perform the process yourself or purchase Oracle installation services.

> **Note:**
>
> These steps assume a new installation. See Upgrade to STA 2.4.0 if upgrading from a previous version.

1. Review Requirements for STA .
2. Review Best Practices for STA Deployment.
3. Prepare Service Requests for the Libraries and Drives (as necessary).
4. Install and Configure Linux on the STA Server.
5. Install STA .
6. Configure SNMP (for SL150, SL500, SL3000, SL8500).
7. Configure additional STA usernames and emails. See the *STA User's Guide*.
8. Configure monitoring and database backup. See the *STA Administration Guide*.
9. Configure Security Certificates (optional).
10. Configure External Authentication Providers (optional).

Best Practices for STA Deployment

Review all best practices before installing STA to optimize the performance of the STA server, database, and application.

- Installation Planning Best Practices
- Linux Installation Best Practices
- STA Installation Best Practices
- Library Configuration Best Practices

- SNMP Connection Best Practices
- Data Collection Best Practices
- STA Services Best Practices

Installation Planning Best Practices

Follow planning guidelines to ensure a smooth STA installation.

Ensure STA is on a dedicated server
To ensure optimal performance and functionality of the STA application, STA must be installed on a dedicated server (called the STA server). There should be no other applications running on the server. Oracle Service can provide support only if these conditions are met.

Get assistance with STA server sizing
Contact your Oracle sales representative for assistance with sizing your STA server. Your sales representative can use the STA Server Sizing Tool to provide you with best sizing recommendations to meet your site's current needs and expected growth. See Server Requirements.

Plan the file system layout
For optimal performance and functionality of the STA application, plan your STA file system layout and space allocations carefully. The file system is configured during Linux installation. See Review the STA File System Layout.

Linux Installation Best Practices

Follow Linux installation guidelines to ensure STA installs on the server.

Enable iptables
Starting with STA 2.3.0, the iptables firewall service must be running. Before beginning an STA installation, you must enable iptables so the installer can set up required port configurations. Once STA is installed, iptables must remain running to support internal port forwarding for SNMP traps. See Enable the Linux Firewall iptables.

Use yum for RPM package updates
Use yum to install Linux RPM packages. yum greatly simplifies the package installation process by automatically searching RPM package repositories for the latest package versions and their dependencies. See Setup yum (optional).

Verify mariadb packages are not installed
The mariadb packages (an alternative to MySQL) must not be installed on the STA server. The package will cause the MySQL installation of STA to fail.

STA Installation Best Practices

Follow STA installation guidelines to ensure STA installs on the server.

Use the latest version of STA
For best system performance and the most robust analytics and reporting, always upgrade to the latest version of STA. See Install STA .

Register the Oracle central inventory
Beginning with STA 2.1.0, the STA installer uses the Oracle central inventory location, which is a convention common to many Oracle products. After completing STA installation, you should register the Oracle central inventory location on the STA server by running the provided registration script. Registering the location will facilitate the installation of future STA upgrades. See Register the Oracle Central Inventory Location.

Do not run browsers on the STA server
For optimal STA server performance, you should not run a browser on the STA server to access the STA user interface or for any other purpose. Run browsers on platforms separate from the STA server. See Ensure Local Browser Functionality (optional).

Library Configuration Best Practices

Follow library configuration guidelines to ensure the tape libraries send data to STA.

Verify library and drive firmware levels
To ensure richer library and drive data, use the most current library and drive firmware levels. See Library Requirements and Tape Drive Requirements.

Set library parameters before installing STA
To ensure complete compatibility with STA, you must set some library parameters to specific values. Make the following changes before configuring the library connection to STA.

- For SL8500 libraries, make sure the complex ID is unique for each monitored SL8500 complex. See Ensure the Correct Library Complex ID (SL8500 only).
- For SL150 and SL500 libraries, ensure the volume label format is set correctly. See Set Element Addressing Mode (SL150 only) and Set Volume Label Format.

Stop library activity before changing library parameters
You should stop all activity on a library before changing any library parameters. In addition, tape applications and hosts may require configuration changes after updating the library parameters.

Avoid duplicate volsers
Because all history for a particular piece of media is tied to its volume serial number (volser), you should avoid duplicate volsers in your tape library environment. See Avoid Duplicate Volume Serial Numbers.

SNMP Connection Best Practices

Follow SNMP guidelines to ensure that the tape libraries send data to STA.

Use SNMP v3
For communication between STA and the monitored libraries, Oracle recommends the more secure SNMP v3 protocol rather than v2c. However, v2c is available to support older library firmware levels. The authentication, encryption, and message integrity features in v3 provide a secure mechanism for sending library data. v3 is also required for STA media validation.

Create a unique SNMP v3 user
Oracle recommends creating a new, unique SNMP v3 user on the libraries for STA communications.

Data Collection Best Practices

Follow data collection guidelines to verify the STA is receiving up-to-date library data.

Test the Library Connection
Certain activities performed in STA or on a monitored library may cause the library connection to drop. To minimize the dropped connection time and prevent the loss of large amounts of data, perform a connection test at the following times:

- After the initial library connection between STA and a library has been configured
- After any STA SNMP client settings have been modified
- After any connection settings for a monitored library have been modified
- After a monitored library has been rebooted or experienced a redundant electronics switch
- Any time the library engine ID field is blank on the Library Connections – Monitored Libraries screen
- After STA has been upgraded

Perform initial library data collections
After configuring STA, you should perform a manual library data collection on each library configured to the STA server. It is recommended that you perform these initial data collections while library activity is low or stopped.

Configure automatic daily library data collections
STA relies on automatic daily library data collections to gather key information for processing exchanges and evaluating the state of the library. Ideally, the daily data collections should be scheduled for times when the library is less busy. It is recommended that you choose the best time for your organization.

Perform manual data collections as-needed
For STA to receive library data, you must perform a manual data collection at the following times:

- After a new library connection has been configured
- After connection settings in STA and on the library have been modified
- After a redundant electronics switch has occurred
- After there have been any hardware configuration changes to the library, including moving drives

STA Services Best Practices

Follow best practices when using STA services to help manage the database.

Configure database backups
You should configure a remote backup server for STA database backups. See the *STA Administration Guide* for instructions.

Manage database backup space usage
It is the customer's responsibility to manage space on the STA remote backup server. You should periodically check the amount of space consumed by the STA database backups and take appropriate action when space is running low.

Configure the STA Resource Monitor on the STA server
To assist with management of the STA server, you can define high water marks for disk and memory usage, and the Resource Monitor will alert you if these are exceeded. See the *STA Administration Guide* for instructions.

Database Tuning Best Practices

Follow database tuning guidelines to maximize the performance of the database.

Database considerations for larger installations
If you have significant library exchanges per hour rates (that is, greater than 300) with multiple libraries attached to a single STA server and a long history with STA, you might need to make adjustments to two InnoDB buffer pool parameters in the MySQL configuration file, `/etc/my.cnf`. To change these parameters, first stop STA, then modify the `my.cnf` file, and then restart STA to activate the new values.
The key parameters that may need adjusting based on your server configuration are as follows.

- `innodb_buffer_pool_size` — 24GB or greater. The value should be 70–80 percent of the STA server's physical memory.
- `innodb_buffer_pool_instances` — 8 minium. More buffer pools improve concurrent processing.

Prepare Service Requests for the Libraries and Drives

To prepare your libraries for monitoring by STA, you may need to provide Oracle support with library and drive information.

1. Verify the Library Firmware Version.
2. Verify the HBT Drive Controller Card Version (SL3000 and SL8500 only).
3. Enable ADI on the Library (SL500, SL3000, SL8500).
4. Ensure the Correct Library Complex ID (SL8500 only).
5. Set the library date and time. To ensure that library data date/time stamps correlate to STA server date/time stamps, the library clock should be set appropriately by Oracle support.
6. Submit the necessary service requests. If STA will be monitoring a library complex, prepare a service request for each library in the complex. Additionally, open a Service Request to install the latest drive firmware supported by STA.

3

Install and Configure Linux on the STA Server

Install and configure a supported version of Linux on the server before installing STA.

> **Note:**
>
> If the server is already running a supported version of Linux, be sure to review the Configure Linux section since there may be new pre-requisites or requirements.

To install and configure Linux for STA, perform the following tasks:

- Prepare for the Linux Installation
- Install Linux
- Configure Linux

Prepare for the Linux Installation

Before installing Linux, review the documentation, review STA requirements, plan the file system layout, and download the Linux installer.

- Review Related Documentation and Requirements
- Review the STA File System Layout
- Download the Linux Installer Media Pack

Review Related Documentation and Requirements

Review related Linux documentation and all STA requirements before proceeding with the installation.

Due to the wide variety of network configuration requirements and options, refer to the Linux documentation to help with installing and configuring the hardware, software, and network.

- Oracle Linux Installation Guides: `http://docs.oracle.com/en/operating-systems/`

Review all Requirements for STA . Make sure your environment meets all requirements before proceeding.

> **Note:**
>
> You cannot do an in-place upgrade of Linux. If you are installing a new version of Linux as part of an upgrade to STA, see Upgrade to STA 2.4.0

Review the STA File System Layout

Review the file system layout recommendations to plan your configuration before installing Linux.

Create the file systems during the Linux installation and ensure that the Oracle user has write privileges to the required file systems before STA installation. The STA installation will fail if the Oracle user does not have proper write privileges.

The table below describes the recommended layout and space allocations for a typical installation. For larger installation, see Server Sizing and Considerations for Larger Installations.

> **Note:**
>
> All directories must be mounted before starting STA (including any auto-mounted directories). For performance reasons, Oracle does not recommend that the `/dbdata`, and `/Oracle` directories use NFS mount points.

Oracle recommends that usage for any partition should never exceed 80 percent. After installing STA, you can configure the Resource Monitor to automatically notify you if usage exceeds a high-water marks. See the *STA Administration Guide* for instructions. You need to periodically check locations not monitored by the Resource Monitor.

Table 3-1 Recommended File System Layout

File System	Default Mount Point	Size	Description and Recommendations
root	/	32 GB min.	root file system. Space requirement is for files and directories critical for system operation. See entries below for additional space requirements if the temp and STA logs directories are also located in this file system.
temp	`/tmp`	11 GB min.	Location of temporary files. At least 4 GB of free space is required in temp for STA installations and upgrades.
STA logs	`/var/log/tbi`	30 GB min. 50 GB to 100 GB suggested	Location of STA logs and STA database binary logs. This location should be a separate volume at a separate mount point. The default location is `/var/log/tbi`, but you can change this location at any time after STA installation; see Relocate the STA Logs Directory (optional) for instructions. **Note**: The contents tend to grow over time. Except for log rotation, STA does not perform space management. **Note:** Incremental database backups (binary files) in `/STA_logs/db` may consume significant space but are purged every 24 hours by the STA backup utility. See the *STA Administration Guide* for details on configuring their frequency.
swap	None. Defined as memory.	50 to 100 percent of RAM size	Used for swap space.

Table 3-1 (Cont.) Recommended File System Layout

File System	Default Mount Point	Size	Description and Recommendations
Oracle storage home	`/Oracle`	30 GB min. 100 GB suggested	Location of the STA and Oracle Middleware (WebLogic, MySQL, RDA) application files. This location is user-defined. This location should be a separate file system on a separate volume. Maintain a minimum of 11 GB free space for STA installations and upgrades. Maintain an additional 5 GB free space for WebLogic log rotation. STA automatically creates the following Oracle Middleware subdirectories: • Rotated WebLogic logs: `/Oracle_storage_home/Middleware/user_projects/domains/TBI/servers` • RDA last CLI snapshot: `/Oracle_storage_home/Middleware/rda/output` • STA GUI snapshot log bundles: `/Oracle_storage_home/Middleware/rda/snapshots`
STA database location	`/dbdata`	250 GB to 2 TB	Location of the STA database. This location is user-defined. Oracle highly recommends you place this directory on its own volume, separate from root, swap, Oracle storage home, and the STA logs location. For performance, backup, and maintainability, best practice is to use a separate set of mirrored or striped drives. Required size depends on the number of libraries, drives, media, exchanges per day, and historical years of data. Oracle recommends that you configure STA services to alert if space utilization exceeds a specified percentage.
STA database local backup location	`/dbbackup`	70 to 80 percent of `/dbdata` size	Location of the most recent local database backup. This location is user-defined. Oracle recommends that this directory be on a different volume from the STA database, and on mirrored or striped drives in case of database corruption or failure.

Download the Linux Installer Media Pack

Download the Linux installer media pack from the Oracle Software Delivery Cloud.

1. Obtain an Oracle Software Delivery Cloud user ID and password from your Oracle support representative.
2. Go to: `http://edelivery.oracle.com/linux`
3. Click **Sign In/Register**. Enter your user ID and password.
4. In the search bar, start typing `Oracle Linux`. Select **Oracle Linux** from the drop-down list.
5. Click **Add to Cart** for the Linux version you want to download.
6. Click **Checkout**.
7. In the Platforms/Languages column, select **x86 64 bit**. Click **Continue**.
8. Review the Terms & Restrictions screen, select the boxes to indicate your acceptance and then click **Continue**.

9. Download the ISO file and save it to a portable media device (such as a flash drive).

Install Linux

Gather all required network information, then run the Linux installer and Setup Agent.

- Gather Required Network Information
- Run the Linux Installer
- Run the Linux Setup Agent

Gather Required Network Information

Contact your system administrator to obtain network configuration information.

- Hostname and IP address for the STA server
- Gateway IP address and netmask for your network
- DNS server IP addresses and search domains for your network
- IP address of the NTP (network time protocol) servers you will be using
- Network proxy information, if applicable

Run the Linux Installer

Install a compatible version of Linux on the STA server by running the corresponding installation package.

1. Complete Download the Linux Installer Media Pack.
2. Connect the installation media (flash drive) to the STA server.
3. Start the Linux installer using the instructions in the README file on the media.
4. Select **Install or upgrade an existing system**.
5. If you are installing from a DVD, the CD Found screen appears. You can optionally perform a test of the media. To skip the test, press **Tab** to highlight the **Skip** option, and then press **Spacebar**.
6. On the Welcome screen, click **Next**.
7. Select a language, and then click **Next**.
8. Select a keyboard layout, and then click **Next**.
9. Select **Basic Storage Devices**, and then click **Next**.
10. Enter a hostname for the STA server, and then click **Configure Network**.
11. Select the network adapter name, and then click **Edit**.
12. Ensure that **Connect automatically** and **Available to all users** are both selected.
13. In the remaining tabs, configure the adapter according to your network administrator's IPv4 or IPv6 specifications. You must specify a static IP address for the STA server, and at least one DNS server. When done, click **Apply**, **Close**, and **Next**.

14. Select the STA server's time zone, select the **System clock uses UTC** check box, and then click **Next**.
15. Enter and confirm a system root password for the server, and then click **Next**.
16. Identify a partitioning layout to use on the server.

    Because STA requires a dedicated server, Oracle recommends selecting **Use All Space**.

    Select the **Review and modify partitioning layout** check box, and then click **Next**.
17. Use the table in Review the STA File System Layout to modify the file system layout, as the default does not meet the minimum requirements for STA. Alternatively, you can use the `system-config-lvm` utility to modify the file system after Linux installation.

    When done, click **Next**.
18. When ready, select **Write changes to disk**.
19. In the boot loader screen, leave all options as-is, and then click **Next**.
20. In the software selection screen, select **Basic Server**, and do not change the repository options. Then, select **Customize now**, and then click **Next**.
21. In the package selection screen you must select or deselect specific packages. Use the table below to configure the packages. Leave other check boxes as-is.

    If a package requires an option (indicated with a +), highlight the parent package, click the **Optional packages** button, select the child package in the list, and then click **Close**.

Table 3-2 Linux Package Selection

Package Category	Select	Deselect
Base System	• Base • Compatibility libraries • Console internet tools • Java Platform • Legacy UNIX compatibility(+ `ksh-xxxxxxxx-xx.el6.x86_64`)	• Debugging Tools • Dial-up Networking Support • Directory Client • Hardware monitoring utilities • Large Systems Performance • Network file system client • Performance Tools
Servers (optional)	• System administration tools	NA
Web Services	NA	All packages
Databases	NA	All packages
System Management	NA	NA
Virtualization	NA	NA
Desktops (recommended)—Used to perform certain post-installation steps in a graphical environment; see Configure Linux for details.	• Desktop • Desktop Platform • General Purpose Desktop (+ `system-config-lvm-x.x.xx-xx.el6.noarch`) • Legacy X Window System compatibility • X11 (X Window System, version 11)	NA

Table 3-2 (Cont.) Linux Package Selection

Package Category	Select	Deselect
Applications (optional)— Can be used to configure and manage the STA server locally with the GUI interface.	• Internet Browser	NA
Development	• Development tools (+ `expect-x.xx.x.xx-x.el6.x86_64`)	NA
Languages	NA	NA

22. When you are finished with package selection, click **Next**. Installation will begin.

    If you accidentally click **Next** before configuring all the packages, click **Back** after the software completes a dependency check.

23. When the Congratulations screen appears, remove the installation media, and then click **Reboot**.

    A complete log of the installation can be found in `/root/install.log`.

Run the Linux Setup Agent

The Linux Setup Agent starts automatically when you reboot the server. Use it to configure the system environment.

1. On the Welcome screen, click **Forward**.
2. Read the License Agreement, select **Yes, I agree to the License Agreement**, and click **Forward**.
3. On the Software Updates screen, if you'd like to register your system for updates, select **Yes, I'd like to register now**. Otherwise, select **No, I prefer to register at a later time**, and click **Forward**.
4. On the Finish Updates Setup screen, click **Forward**.
5. On the Create User screen, leave the fields blank, click **Forward**, and then **Yes** to continue. The STA server does not require a non-administrative user.
6. In the Date and Time screen:
   a. Set the current date and time.
   b. Select the **Synchronize date and time over the network** check box.
   c. Add or remove the desired NTP servers (obtained from your IT administrator), and then click **Forward**.

   > **Note:**
   >
   > To ensure that STA data and log files are correct, the date and time on the STA server must be correct. Additionally, any library connected to STA must also have the correct time.

7. On the Kdump screen, do *not* select **Enable kdump?**. Then click **Finish**.

   The system reboots.

8. After the system reboots, log in as the system root user:
   a. Click **Other...**.
   b. Enter username **root**, and then click **Log In**.
   c. Enter the system root password, and then click **Log In** again.
   d. If a message appears about being logged in as root super user, you may ignore the message.
9. Confirm the Linux release and update level. This step is optional.

```
# cat /etc/*-release
```

Configure Linux

Configure Linux to prepare the server for the STA installation. If the Linux environment is not properly setup, the STA installation will fail.

Perform the following in order:

- Verify the root User Path
- Enable the Linux Firewall iptables
- Disable SELinux
- Remove SELinux Permissions
- Set Up the Network Proxy
- Setup yum (optional)
- Install Required Linux Packages
- Setup SSH
- Configure DNS Settings
- Disable Name Services
- Ensure Local Browser Functionality (optional)

Verify the root User Path

Verify the path for the system root user. The path must be configured correctly for the STA installation.

1. Open a terminal session on the STA server and log in as the system root user.
2. Display the `PATH` variable and verify that it includes all the following directories:

```
/bin
/sbin
/usr/bin
/usr/sbin
```

For example:

```
# echo $PATH
/usr/lib64/qt-3.3/bin:/usr/local/sbin:/usr/local/bin:/root/bin:/sbin:/bin:/usr/
sbin:/usr/bin
```

3. If any directories are missing, use a text editor to open the user profile and add them. For example:

```
# vi /root/.bash_profile
PATH=$PATH:/sbin:/bin:/usr/sbin:/usr/bin
```

   Save and exit the file.

4. Log out and log in as the system root user.
5. Confirm that the `PATH` variable has been updated correctly.

```
# echo $PATH
/usr/lib64/qt-3.3/bin:/usr/local/sbin:/usr/local/bin:/root/bin:/sbin:/
bin:/usr/sbin:/usr/bin
```

Enable the Linux Firewall iptables

Enable the iptables firewall service so the STA installer can set up required port configurations. Once STA is installed, iptables must remain running to support internal port forwarding for SNMP traps.

1. Open a terminal session on the STA server and log in as the system root user.
2. Enable the iptables:
   a. Check the current status of the iptables service.

```
# systemctl status iptables
```

   b. If the firewall is not running, start and enable it.

```
# systemctl start iptables
# systemctl enable iptables
```

Disable SELinux

STA does not support SELinux. Disable SELinux before installing STA.

1. Open a terminal session on the STA server and log in as the system root user.
2. Open the SELinux configuration file with a text editor.

```
# vi /etc/sysconfig/selinux
```

3. In the file, set `SELINUX` to `disabled`:

```
SELINUX=disabled
```

4. Save and exit the file.
5. Reboot the STA server to make your changes take effect.

Remove SELinux Permissions

Remove SELinux permissions for directories created before you disabled SELinux.

This is important if you did not just freshly install Linux. In particular, the Oracle storage home, STA database, STA database local backup, and STA logs locations must not have SELinux permissions.

1. Open a terminal session and log in as the system root user.

2. List permissions for the Oracle storage home, STA database, STA database local backup, and STA logs locations. In a brand-new Linux installation these directories likely do no exist yet, but you should verify.

   For example:

   ```
   # ls -ld /Oracle /dbdata /dbbackup /var/log/tbi

   drwxr-xr-x. 2 oracle oinstall  4096 Jul 30 14:48 /Oracle
   drwxr-xr-x. 3 root   root  4096 Jul 30 14:46 /dbdata
   drwxr-xr-x. 3 root   root  4096 Jul 29 14:13 /dbbackup
   drwxrwxrwx. 4 root  root 4096 Jul 30 14:46 /var/log/tbi
   #
   ```

3. In the output for each command, look for a dot at the end of the permissions. In the following example, note the "." after `drxwr-xr-x`.

   ```
   # ls -ld /Oracle

   drxwr-xr-x.  5  oracle oinstall  4096  Jul  30  18:27  /Oracle
   ```

4. If none of the directories contain a dot after the permissions statement, SELinux permissions have not been assigned to the directories and you can proceed to the next task.

   If SELinux permissions are assigned to a directory, enter the following command for that directory.

   ```
   # setfattr -h -x security.selinux directory_name
   ```

   For example:

   ```
   # setfattr -h -x security.selinux /Oracle /dbdata /dbbackup /var/log/tbi
   ```

5. Confirm that the SELinux permissions have been removed.

   ```
   # ls -ld /Oracle /dbdata /dbbackup /var/log/tbi

   drwxr-xr-x 2 oracle oinstall  4096 Jul 30 14:48 /Oracle
   drwxr-xr-x 3 root   root  4096 Jul 30 14:46 /dbdata
   drwxr-xr-x 3 root   root  4096 Jul 29 14:13 /dbbackup
   drwxrwxrwx 4 root  root 4096 Jul 30 14:46 /var/log/tbi
   #
   ```

Set Up the Network Proxy

Configure the STA server to connect to the network directly or through a proxy server.

1. From the Linux desktop **System** menu, select **Preferences**, then select **Network Proxy**.
2. In the Network Proxy Preferences dialog box, specify the proxy configuration according to your site requirements.
3. Click **Close**.

Setup yum (optional)

Oracle recommends you use yum (Yellowdog Updater, Modified) to install the required RPM (Red Hat Package Manager) Linux software packages.

yum simplifies the installation process by automatically searching RPM package repositories for the latest package versions and their dependencies. See Install Required Linux Packages for the required packages.

Use this procedure to ensure that yum is configured correctly on the STA server.

> **Note:**
>
> The command examples use `ol7` where the "`l`" is lower-case "`L`".

1. Ping the Oracle public-yum server to ensure the network connection is working.

   ```
   # ping public-yum.oracle.com
   ```

2. Change to the yum repository directory and determine the yum repository filename.

   ```
   # cd /etc/yum.repos.d
   # ls
   public-yum-ol7.repo
   ```

3. Remove the existing yum repository file.

   ```
   # rm public-yum-ol7.repo
   ```

4. Download the latest yum repository file from the yum website.

   ```
   # wget http://public-yum.oracle.com/public-yum-ol7.repo
   ```

   > **Note:**
   >
   > Subsequent executions of this command will copy a new repository file into the `yum.repos.d` folder with a new extension (for example, `public-yum-ol7.repo.1`). However, yum always uses the repository file with no extension.

5. Open the repository file with a text editor.

   ```
   # vi public-yum-ol7.repo
   ```

6. In the file, locate the entry that matches your Linux version and enable it by setting `enabled=1`. Disable all other entries by setting `enabled=0`.

   For example:

   ```
   [Linux_Version]
   name=Oracle Linux $releasever Update x installation media copy ($basearch)
   baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL7/x/base/$basearch/
   gpgkey=http://public-yum.oracle.com/RPM-GPG-KEY-oracle-ol7
   gpgcheck=1
   enabled=1
   ```

7. Save and exit the file.

Install Required Linux Packages

STA requires additional RPM packages. The STA installer will check for specific packages and if they are not present, the STA installation will fail.

> **Note:**
>
> RPM package names are case-sensitive. Choose the 64-bit version (x86_64) of any package if more than one version is available.

Required RPM Packages

- bc
- binutils
- compat-libcap1
- compat-libstdc++-33
- cronie
- ed
- expect
- gcc
- gcc-c++
- glibc
- glibc-devel
- libaio
- libaio-devel
- libgcc
- libstdc++
- libstdc++-devel
- net-snmp-utils
- net-tools
- perl-Data-Dumper
- perl-Digest-MD5
- perl-Digest-SHA
- rpm-build
- sysstat
- unzip
- xorg-x11-xauth
- xorg-x11-utils

Packages that must NOT be installed

The mariadb packages (an alternative to MySQL) must NOT be installed on the STA server as it will cause the MySQL installation to fail.

Mail Services Packages

The STA installer issues a warning if it does not detect a package that supports mail services. STA requires mail services to deliver email notifications for alerts or Resource Monitor threshold notices.

The installer checks for the following: mailx, sendmail, postfix, dovecot.

IMPORTANT: The postfix mail package is NOT acceptable if it has a dependency on the mariadb-libs package.

Using yum to manage the packages

You can use a variety of methods to install the required RPM packages. This procedure describes how to use yum. See Setup yum (optional).

Deinstalling Packages

To de-install the mariadb-libs package (which may have been installed as a dependency):

```
# yum remove mariadb-libs
```

This will also remove any dependent packages, including postfix if necessary.

Installing Packages

yum checks for the most current version and then installs the package and any dependencies. Depending on your Linux installation, some of these packages may have already been installed. If a package is already installed and at the most current version, the system notifies you.

1. Open a terminal session on the STA server.
2. If you can reach Oracle's public yum server, use one of the following methods to install packages:
   - Install packages one at a time.The specified package will be downloaded and checked, and you must answer all prompts.

     ```
     # yum install package_name
     ```

   - Install all packages at once with no prompting. The `-y` option automatically answers "yes" to all installation prompts.

     ```
     # yum -y install bc binutils compat-libcap1 compat-libstdc++-33 cronie
     ed expect gcc gcc-c++ glibc glibc-devel libaio libaio-devel libgcc
     libstdc++ libstdc++-devel net-snmp-utils net-tools perl-Data-Dumper perl-
     Digest-MD5 perl-Digest-SHA rpm-build sysstat unzip xorg-x11-xauth xorg-
     x11-utils
     ```

3. If your network firewall prohibits external network access, you can use yum to install locally available packages from the Linux media.

   For example:

```
# cd /mnt/install_media_mount_location/packages
# yum install ./package_name
```

Setup SSH

Correctly setup the SSH (secure shell) on the STA server. This will speed up transfers of STA database backups to a remote host.

1. Open the SSH configuration file with a text editor.

   ```
   # vi /etc/ssh/sshd_config
   ```

2. Search for the `AddressFamily` and `UseDNS` entries. Modify them so they are *not* preceded with the comment character and their values are as follows:

   ```
   AddressFamily inet
   UseDNS no
   ```

3. Save and exit the file.
4. Restart the sshd daemon.

   ```
   # systemctl restart sshd
   ```

Configure DNS Settings

Map the STA server's IP address to its hostname.

1. Open the hosts file with a text editor.

   ```
   # vi /etc/hosts
   ```

2. At the end of the file, add the STA server's IP address, followed by a tab, and then the STA server's hostname. For example:

   ```
   127.0.0.1    localhost localhost.localdomain localhost4...
   ::1          localhost localhost.localdomain localhost6...
   192.0.2.20    sta_server
   ```

3. Save and exit the file. You do not need to restart the STA server for the new setting to take effect.

Disable Name Services

Name services (such as LDAP) can conflict with STA installation. Temporarily disable these services during STA installation and do not use an LDAP defined user for the Oracle user.

1. Open the Name Service Switch configuration file with a text editor.

   ```
   # vi /etc/nsswitch.conf
   ```

2. Disable any name service entries. For example, to disable LDAP, comment out "ldap" from the following lines as shown:

   ```
   passwd:     files #ldap nis nisplus
   shadow:     files #ldap nis nisplus
   group:      files #ldap nis nisplus
   ```

3. Save and exit the file. You do not need to restart the STA server for the new setting to take effect. After you install STA, you can modify the nsswitch.conf file to re-enable the name services.

Ensure Local Browser Functionality (optional)

To configure and administer STA locally on the STA server, ensure you have the minimum supported browser versions and plugins installed on your workstation.

Review the User Interface Requirements.

If you will be using HTTPS to access STA, see the *STA User's Guide* for instructions on ensuring that HTTPS is supported by your browser.

Oracle does not recommend local access to the STA application due to server performance degradation.

4
Install STA

Install STA after installing Linux. Oracle provides support only if STA is installed on a dedicated server (meaning the server is not running any other applications). The server can only have one instance of STA installed.

- What is Configured During STA Installation
- Install STA
- Logs Created During Installation, Upgrade, and Deinstallation
- Troubleshoot the Installation

These instructions assume you are installing STA on the server for the first time. For upgrades or to reinstall or repair a current installation, see:

- Upgrade to STA 2.4.0.
- Deinstall and Restore STA.

What is Configured During STA Installation

Before installing STA, understand what the STA installation configures.

- Users, Groups, and Locations Used by the STA Installer
- Administration and Database Accounts Created During STA Installation
- Ports Configured During STA Installation

Users, Groups, and Locations Used by the STA Installer

The STA installation configures specific users, groups, and directories. Understand how these are used by STA so that you will know how best to configure them during installation.

Pay close attention to the ownership and permissions required for each location. Make sure that the locations do not have SELinux permissions. See Remove SELinux Permissions.

Oracle group
The Linux group used for installing and upgrading Oracle products on the STA server. Oracle recommends creating a separate group dedicated for this purpose. To perform STA installation and administration, you must log in as a user that is a member of this group. You cannot install STA as the Linux `root` user nor any other user with superuser privileges
The instructions and examples in this guide use the name `oinstall` for this group.

Oracle user
The Linux user used to install Oracle products on the STA server, run STA utilities, and run the STA application. This can be any user that is a member of the Oracle group. Depending on your site's configuration, some of the activities performed by this user may require system root privileges. The administrator should add the Oracle user to the system sudoers file if this is the case.

Do not use an LDAP defined user for the Oracle user.
The instructions and examples in this guide use the name `oracle` for this user.

Oracle central inventory location
The directory used for tracking information about Oracle products installed on the STA server. The `logs` subdirectory within this location contains the STA installer and deinstaller logs .
The Oracle user must own this directory and have full permissions to it. Do not use the Oracle user's home directory for this purpose. Other users in the Oracle group need access to this directory so they can install Oracle products. Additionally, do not create any system links in this directory, as these can interfere with an STA installation or upgrade.
Keep this location separate from the other directories described in this section. You should register this location after completing the STA installation so all Oracle installers use the same central inventory location on this server. See Register the Oracle Central Inventory Location for details.
The instructions and examples in this guide use `/opt/oracle/oraInventory` for this location.

Oracle storage home location
The directory used to install STA and associated Oracle software. STA automatically installs in the `StorageTek_Tape_Analytics` subdirectory within this location. Keep this directory separate from the other directories described in this section.
If you are upgrading from an earlier version of STA, this directory may already exist. If so, you should verify the correct ownership and permissions. The Oracle group (not root) must own this directory. The Oracle user must have full permissions the directory. If this directory does not exist, the STA installer will automatically create it if the Oracle user has full permissions to the parent directory.
The instructions and examples in this guide use `/Oracle` for this location.

STA home
The directory where the installer places all STA software. The installer automatically creates this directory within the Oracle storage home location and names it `StorageTek_Tape_Analytics`.
The instructions and examples in this guide use `/Oracle/StorageTek_Tape_Analytics` for this location.

STA installer location
The directory where you download the STA installer. Keep this directory separate from the other directories described in this section.
The instructions and examples in this guide use `/Installers` for this location.

STA installer working location
The STA and WebLogic installer files unpack to the `STA_home/tmp` directory, which requires a minimum 11 GB of space. You can unpack the STA installer files to a different working location by running the STA installer with the following option:
`-J-Djava.io.tmpdir=<absolute path for working directory>`
For example:

```
$ ./sta_installer_linux64.bin -J-Djava.io.tmpdir=/Oracle/tmp
```

STA logs location
The default location of the STA and MySQL logs is `/var/log/tbi`, but you can change this location at any time after STA installation (see Relocate the STA Logs Directory (optional) for instructions. See Review the STA File System Layout for space

requirements. The contents tend to grow. STA manages the log size by rotating the logs.

Administration and Database Accounts Created During STA Installation

The STA installation creates specific administration and database accounts. These accounts are specific to STA (they are not Linux usernames).

STA and third-party applications use the database accounts to access and manage the STA database. These accounts must exist for normal STA operations, but you will not need to log in to any of them.

You can change the passwords for these accounts at any time using the STA Password Change Utility. See the *STA Administration Guide* for details.

WebLogic administrator
Account for logging into the WebLogic Administration console to configure and manage the WebLogic environment—for example, to connect WebLogic to an LDAP or RACF server. This account is used infrequently.

STA administrator
An STA user with administrator privileges created during the installation. This account can log in to the STA user interface with full access privileges. This user can create and manage other user interface accounts (see the *STA User's Guide*).

Database root user
A MySQL account that owns the STA database. It is used internally by the STA application to create the database and provide full access to all database tables. The username for this account is automatically set to `root` and cannot be changed. This is separate from the system root user.

Database application user
A user-defined MySQL account (for example `stadb`) used internally by the STA application to connect to and update the STA database. It provides create, update, delete, and read access to all database tables.

Database reports user
A user-defined MySQL account (for example `starpt`) used by non-STA and third-party applications to connect to the STA database. It provides read-only access to selected database tables.

Database administrator
A user-defined MySQL account (for example `stadba`) used internally by STA utilities to connect to the database and configure and run backups. It provides full access, except the "grant" option, to all database tables.

mysql user
An internal MySQL account that is automatically created during STA installation. It has full create, update, and delete privileges to the database. The username is automatically set to `mysql` and cannot be changed.
Do not modify the credentials for this account, as it may affect the ability of STA to access the database. Unlike the other database accounts, you cannot change its credentials through STA.

Ports Configured During STA Installation

You will configure ports during the STA installation. These are dedicated ports that must remain available to STA. The installer will verify that the ports are not already in use on the network.

See the *STA Administration Guide* for a complete list of ports and for instructions on changing the configurable ports after installation using the Port Change Utility.

The typical port configuration is:

Type	Typical Port
WebLogic Admin Console HTTP	7019
WebLogic Admin Console HTTPS	7020
staEngine HTTP	7023
staEngine HTTPS	7024
staAdapter HTTP	7025
staAdapter HTTPS	7026
staUI HTTP	7021
staUI HTTPS	7022
SNMP Trap Redirection Port	7027

Install STA

Installing STA involves multiple procedures. You must complete them in the order listed.

1. Identify or Create Information Required for the Installation
2. Verify Installation Prerequisites
3. Download the STA Installer
4. Unzip the STA Installer
5. Run the STA Installer
6. Verify Successful Installation
7. Relocate the STA Logs Directory (optional)
8. Register the Oracle Central Inventory Location

Identify or Create Information Required for the Installation

Identify and, if necessary, create users and locations to run the STA installer.

1. Review the information in Users, Groups, and Locations Used by the STA Installer to understand the users and locations needed for the STA installer.
2. On the STA server, open a terminal session. Log in as the system `root` user.
3. Determine if there is an Oracle central inventory pointer file `/etc/oraInst.loc`.

```
# cat /etc/oraInst.loc
```

- If the file exists, you will likely need to identify and record information as outlined in the following steps.
- If the file does not exist, you will likely need to create users and locations as outlined in the following steps.

4. Identify or create the Oracle group.

```
# groupadd oinstall
```

5. Identify or create the username and password of the Oracle user. Do not use an LDAP defined user. This user must belong to the Oracle group.

```
# useradd -g oinstall -d /home/oracle oracle
# passwd oracle
```

Depending on your site configuration, some of the activities performed by this user may require system root privileges. You should add the user to the system sudoers file.

6. Identify or create the Oracle central inventory location. This directory must be owned by the Oracle user.

```
# mkdir -p /opt/oracle/oraInventory
# chown oracle /opt/oracle/oraInventory
# chgrp oinstall /opt/oracle/oraInventory
# ls -la /opt/oracle/oraInventory
```

7. Identify or create Oracle storage home location. This directory must have at least 11 GB of free space. It must be owned by the Oracle user and Oracle group.

```
# mkdir /Oracle
# chown oracle /Oracle
# chgrp oinstall /Oracle
```

8. Identify or create the STA installer location. For example:

```
# mkdir /Installers
```

9. Obtain the password for the system root user. The STA installer requires root access to perform certain tasks and will prompt for the password.
10. Choose usernames for the WebLogic Administrator, STA Administrator, and MySQL accounts that will be created during the installation.
11. Choose port numbers for the configurable internal and external ports required for STA operations. Ensure that the external ports are open on the required networks.
12. Obtain your site's domain name for configuring Oracle's Remote Diagnostics Agent (RDA). See the *STA User's Guide* for details.

Verify Installation Prerequisites

Verify prerequisites before running the STA installer. The installation will fail if any of these prerequisites are not met.

The STA installation assumes 64-bit Linux has been installed with the Linux RPM packages specified in Install Required Linux Packages. If a required package is not installed, the STA installation will display an error message and not allow you to continue until the package is installed. See Requirements for STA for a complete list of installation requirements.

1. Before choosing to permanently remove or replace existing software, back up files as needed.
2. On the STA server, open a terminal session. Log in as the Oracle user.

3. Verify that STA is not installed on the server. For example:

```
$ ls /etc/init.d/sta*
ls: cannot access /etc/init.d/sta*: No such file or directory
$ ls /usr/bin/STA
ls: cannot access /usr/bin/STA: No such file or directory
```

   If STA is already installed, you must deinstall it and then install the new version of STA and then upgrade the database. See Upgrade to STA 2.4.0 for details.

4. Verify that MySQL is not installed on the STA server. For example:

```
$ ls /etc/init.d/mysql*
ls: cannot access /etc/init.d/mysql*: No such file or directory
$ ls /usr/bin/mysql*
ls: cannot access /usr/bin/mysql*: No such file or directory
```

   If MySQL is already installed, you must deinstall it before you can install STA.

5. Verify that the `/tmp` directory has at least 4 GB of free space. For example:

```
$ df -H /tmp
Filesystem             Size   Used  Avail Use% Mounted on /dev/mapper/vg_tbivb03-
lv_root        53G    35G    16G  70% /
```

6. Verify that the Oracle storage home location has at least 11 GB of free space. This is the default STA and WebLogic installer working location. For example:

```
$ df -H /Oracle
Filesystem             Size   Used  Avail Use% Mounted on /dev/mapper/vg_tbivb03-
STA_OracleVol  34G   3.8G    29G  12% /Oracle
```

   If the directory does not have enough space, you can optionally specify a different working directory when you start the STA installer. See STA installer working location for details.

7. Verify SELinux is disabled.

```
$ sestatus
SELinux status:         disabled
```

8. Verify the iptables firewall service is running. Depending on your site configuration, this step may require system root privileges.

   Linux 6:

```
$ sudo service iptables status
```

   Linux 7:

```
$ systemctl status iptables
```

9. Stop and deconfigure SNMP services.

   To avoid network port collisions and other issues, the STA server must not run other SNMP services. The STA installer will quit in the following situations:

   - The snmpd and snmptrapd daemon services are running,
   - UDP ports 161 (SNMP) and 162 (SNMPTRAP) are not available.

   Perform the following steps as required to stop the SNMP services:

   a. Display the current status of the SNMP `snmpd` and `snmptrapd` services.

      Linux 6:

```
$ service snmpd status
$ service snmptrapd status
```

Linux 7:

```
$ systemctl status snmpd
$ systemctl status snmptrapd
```

b. If necessary, stop the SNMP services immediately.

Linux 6:

```
$ service snmpd stop
$ service snmptrapd stop
```

Linux 7:

```
$ systemctl stop snmpd
$ systemctl stop snmptrapd
```

If you receive a "FAILED" error, the services may already be stopped.

c. Disable the SNMP services in the Linux services configuration file so they do not start automatically when Linux reboots. Depending on your site configuration, this step may require system root privileges.

Linux 6:

```
$ sudo chkconfig snmpd off
$ sudo chkconfig snmptrapd off
```

Linux 7:

```
$ systemctl disable snmpd
$ systemctl disable snmptrapd
```

10. Review and verify the applicable mode-specific requirements, as follows:
    - For the installation wizard, see Installation Wizard Display Requirements.
    - For the silent-mode installer, see Silent-mode Requirements.

Download the STA Installer

Download the STA installation package from the Oracle Software Delivery Cloud.

1. Go to the Oracle Software Delivery Cloud: `http://edelivery.oracle.com/`
2. **Sign In** or **Register**.
3. In the search field, enter `StorageTek Tape`. Select select **StorageTek Tape Analytics**.
4. Click **+Add to Cart** for the release you want to download.
5. Click **View Cart/Checkout**.
6. Verify the release level is correct, then click **Continue**.
7. Read and accept the terms/restrictions. Click **Continue**.
8. Download all parts of the STA installation package (for example 1of2 and 2of2).
9. If prompted, install the Download Manager.
10. Save the STA download package to an accessible location.

The download package files include the following, where `version` is the STA installation version number.

- `sta_install_version_linux64.bin`—Required for all installations.
- `sta_install_version_linux64-2.zip`—Required for all installations.
- `silentInstallUtility_version.jar`—Response file build utility. Required only if you will be using the silent-mode installer or deinstaller.

Unzip the STA Installer

Unzip the download package to the installation directory.

Unzip only the top-level zip files (for example, `V76699-01of2.zip`). Do not unzip any files contained within these files (for example, `sta_install_2.1.1.9.16_linux64-2.zip`).

1. Unzip the STA installer to the installation directory created earlier. For example:

```
$ unzip V76699-01_1of2.zip -d /Installers
$ unzip V76699-01_2of2.zip -d /Installers
```

2. Ensure that the Oracle user has all of the following permissions:
   - Ownership of the installation files
   - Execute permissions to the `sta_install_version_linux64.bin` file
   - Read access to `sta_install_version_linux64-2.zip` file and `silentInstallUtility_version.jar` files
3. Review the *Release Notes*, which are included in the installer download package.

Run the STA Installer

Begin the installation by launching either the installation wizard or the silent mode installer.

1. On the STA server, open a terminal session. Log in as the root user.
2. Clear as much space as possible in the system temporary directory (`/tmp`). Remove all files and directories owned by the Oracle user, which may be left over from previous STA installations or installation preparation activities.

```
$ rm -rf /tmp/*
```

3. Switch to the Oracle user. Change to the STA installer location. For example:

```
$ cd /Installers
```

4. Launch the STA installer with one of the following commands:
   - **Installation Wizard (recommended)**— See Install STA with the Installation Wizard. This mode provides a graphical user interface for installing STA. It requires an X11 display.

     ```
     $ ./sta_install_<sta version>_linux64.bin
     ```

     For example:

     ```
     $ ./sta_install_2.3.1_linux64.bin
     ```

- **Silent Installer** — Silent mode allows you to bypass the graphical user interface and supply the installation options in an XML properties file called the *response file*. This mode is useful for unattended installations and for installing STA on multiple machines. By using a response file, you can supply a single set of parameters and automate the installation. You can run the silent-mode installer either from a script or from the Linux command line.

  ```
  $ ../sta_install_<sta version>_linux64.bin -silent  -responseFile <absolute path to response file>
  ```

  For example:

  ```
  $ ./sta_install_2.3.1_linux64.bin -silent -responseFile /Installers/SilentInstall.rsp
  ```

  Before using this mode, you must also download the `silentInstallUtility_version.jar` file and create a response file specifying the installation options.

  See Silent-mode Installer for instructions.

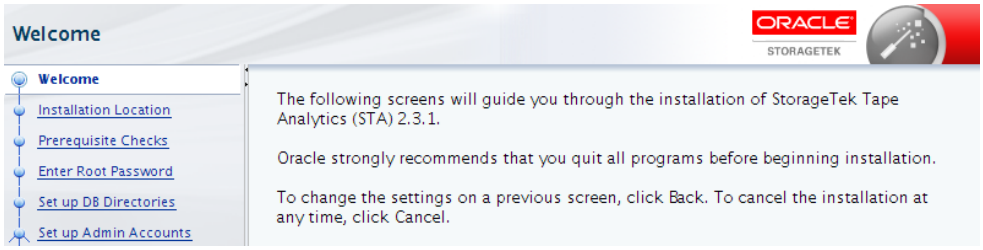
Install STA with the Installation Wizard

Install STA by completing the prompts within the installation wizard.

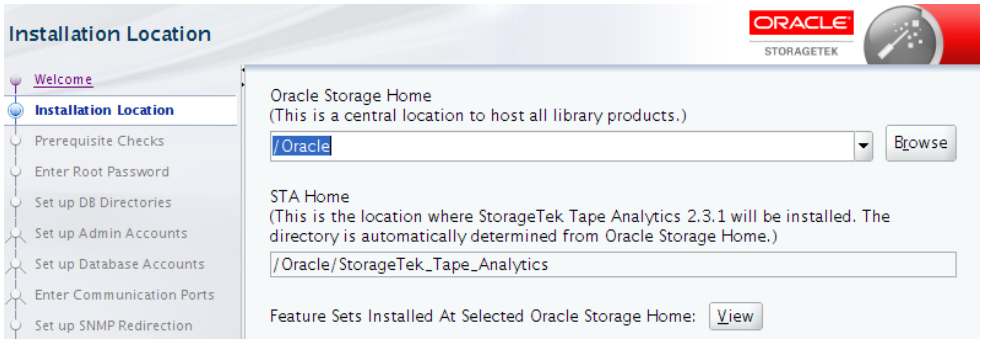
> **Note:**
>
> System changes are not implemented until you complete all the installer screens and click **Install** on the summary screen. Anytime before then, you can return to a previous screen and modify your entries.

1. Before running the installer, review the following to familiarize yourself with what you will configure during the installation:
   - Users, Groups, and Locations Used by the STA Installer
   - Ports Configured During STA Installation
2. Launch the installer by following the instructions in Run the STA Installer.
3. On the *Installation Inventory Setup* screen:
   - Central Inventory Directory — Enter an absolute path or click **Browse** to navigate to the directory to use for the Oracle Central Inventory directory (see Oracle central inventory location). For example `/opt/oracle/oraInventory`.
   - Operating System Group — Enter the Linux group that will have write permissions to the central inventory group (see Oracle group). For example `oinstall`.

4. Review the *Welcome* screen, then click **Next**.

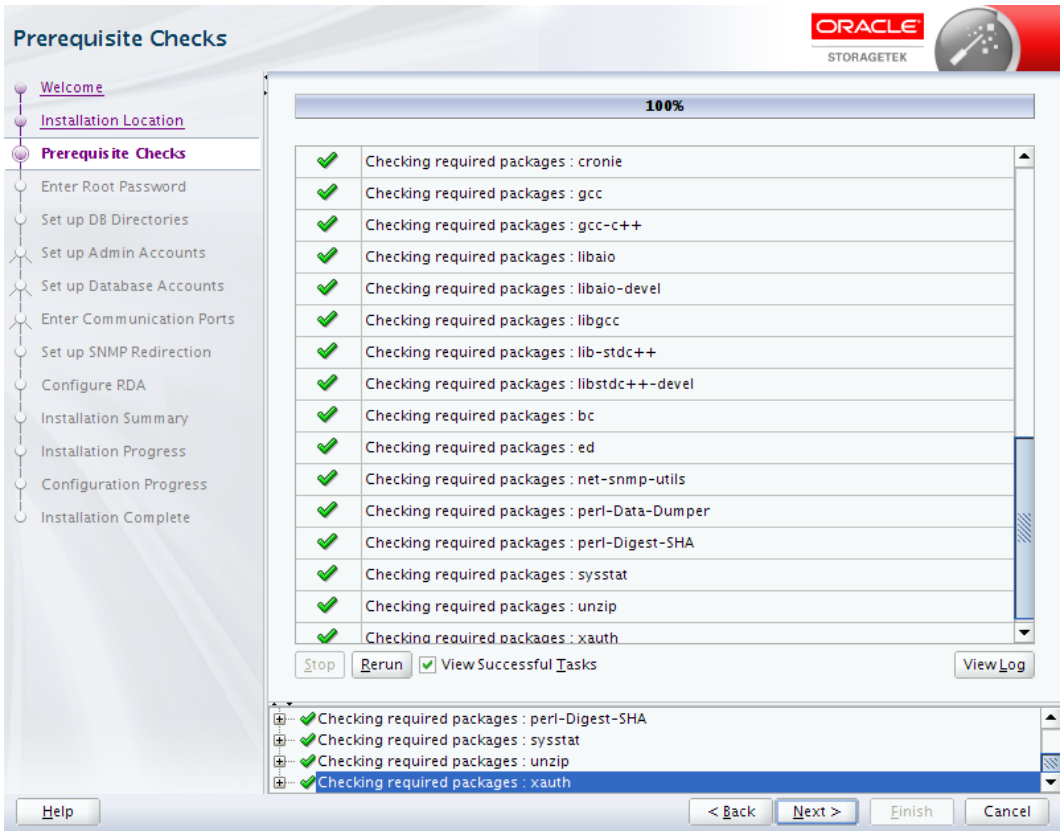


5. On the *Installation Location* screen:



- Oracle Storage Home — Enter an absolute path or click **Browse** to navigate to the directory where STA and associated Oracle software will be installed. For example, `/Oracle`.
  - If the directory already exists, the Oracle user and group must have full permissions to it.
  - If the directory does not exist, the Oracle user and group must have full permissions to the parent directory, so the STA installer can create the Oracle Storage Home directory.
- STA Home — This cannot be changed. This is the subdirectory within Oracle Storage Home where STA will be installed. This subdirectory is assigned the name `StorageTek_Tape_Analytics` and it will be created automatically during the installation.
- View — Click this button to display a list of all software currently installed in the Oracle Storage Home directory you have specified.

6. On the *Prerequisite Checks* screen, the installer performs a series of checks which may take several minutes.



The possible outcomes of each verification test are:

- Success ✔—The prerequisite passed successfully.
- Warning ⚠—The recommended prerequisite did not pass.
- Failure ⊗—The required prerequisite did not pass.

You cannot continue the installation if there are any Failures. You should resolve all Warning outcomes before continuing. You can keep the installer up at this screen while you resolve any issues, and then click **Rerun** to run the verification process again.

Depending on the nature of a prerequisite, you may need to stop a service, change user privileges, or install a yum package to resolve issues. Click a task in the main window. The task is highlighted in the Message pane with expanded detail.

7. On the *Enter Root Password* screen, enter the existing system root password.
8. On the *Set up DB Directories* screen, enter:
   - Database Data Location — the absolute path to the directory where the STA database will be located (for example `/dbdata`).
   - Database Backup Location — the absolute path to the directory where the STA database backups will be located (for example `/dbbackup`). This cannot be the same as the database data location.

9. Review the *Set up Admin Accounts* screen, then click **Next**. Follow the prompts to enter the username and passwords for each of the following users.
   - WebLogic Administrator
   - STA Administrator

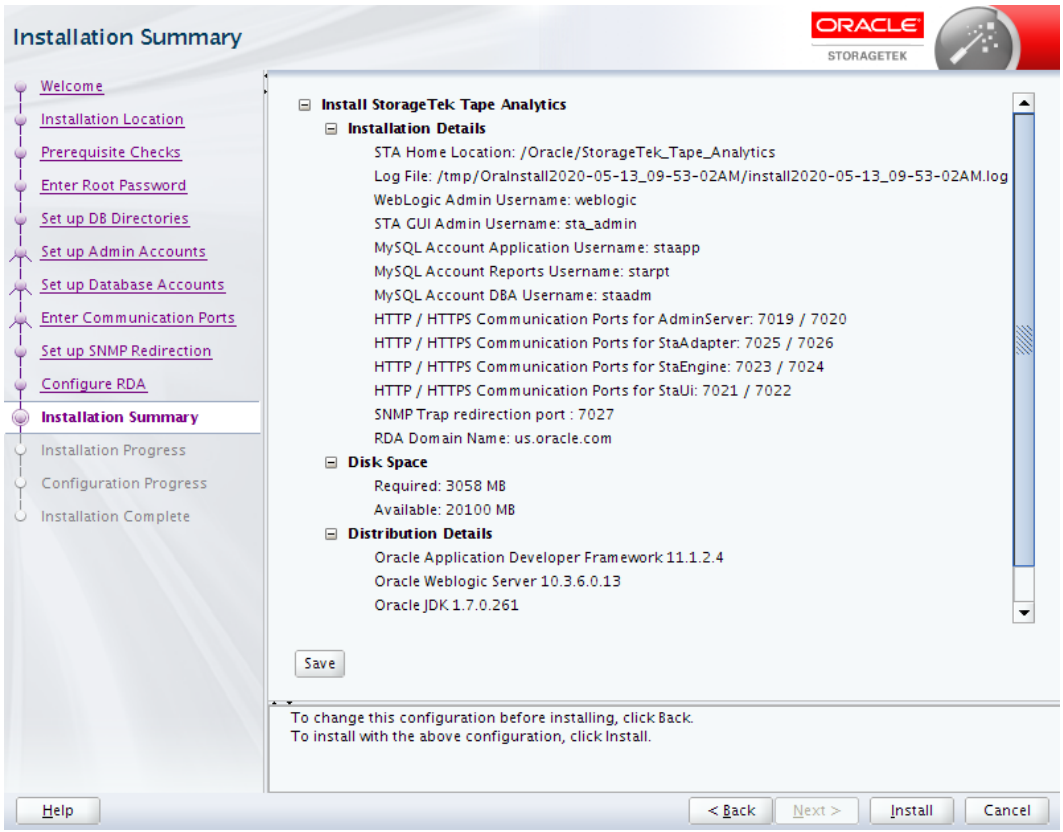
   > **Caution:**
   >
   > Make a secure record of the account credentials (passwords) you create. If you lose them, you will not be able to login and must re-install STA.

10. Review the *Set up Database Accounts* screen, and then click **Next**. Follow the prompts to enter the username and passwords each of the following users:
    - Database Root User
    - Database Application User
    - Database Reports User
    - Database Administrator
11. Review the *Enter Communication Ports* screen, then click **Next**. Follow the prompts to enter the ports for the following:
    - WebLogic Admin Console
    - STA Engine
    - STA Adapter
    - STA UI

    The typical ports used are listed in Ports Configured During STA Installation.
12. On the *Set up SNMP Redirection* screen, enter the redirection port used for SNMP traps.
13. On the *Configure RDA* screen, enter your site's fully qualified domain name. For example, `us.example.com`.

    STA uses RDA to take snapshots of all logs related to the STA application and database, including operating system, installation, and configuration information.
14. Review the *Installation Summary* screen.

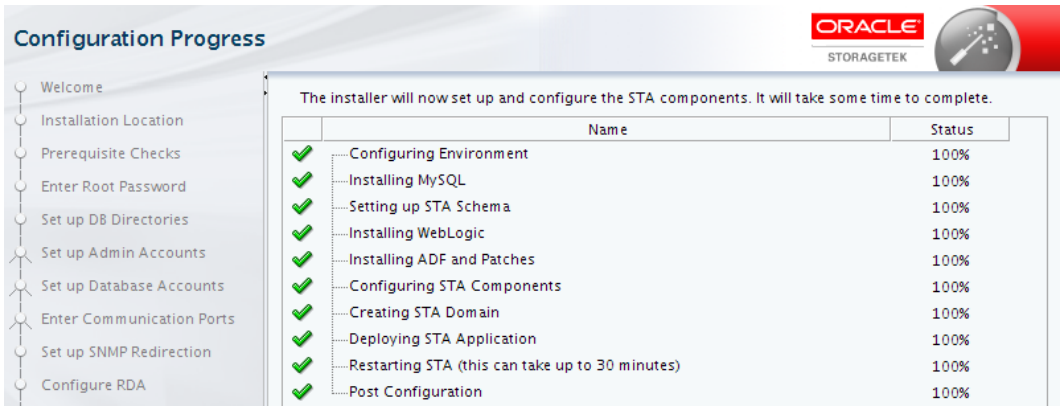
    > **Note:**
    >
    > Once you click **Install**, you cannot pause or cancel the installation.



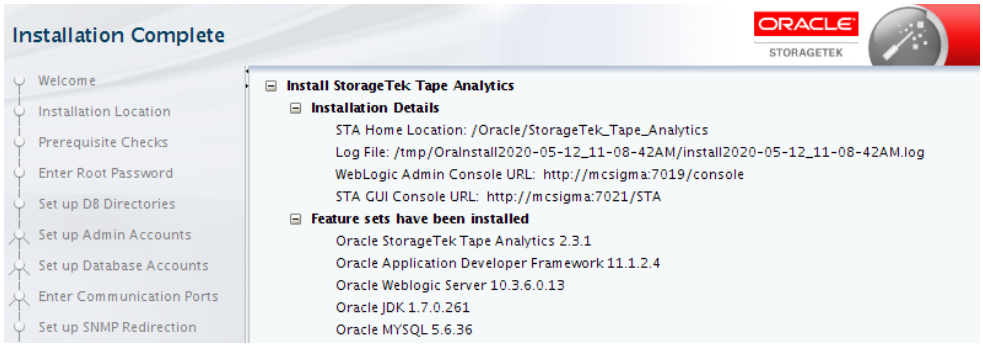
Optionally, click **Save** to save the installation details to a .txt file. Once you are ready to install STA, click **Install**.

15. The *Installation Progress* and *Configuration Progress* screens will display the current status of the installation. Configuration can take 30-60 minutes to complete.

> **Note:**
>
> Do not close this window or interrupt the installation, as this may leave incomplete installation components on the server.



16. Once the *Installation Complete* screen displays, you can click **Finish**.



Verify Successful Installation

Verify that STA is running to make sure the installation was successful.

1. Verify the STA bin directory is included in the `PATH` variable for the Oracle user.
   a. On the STA server, open a terminal session. Log in as the Oracle user.
   b. Open the Oracle user profile using a text editor. For example:

      ```
      $ vi /home/oracle/.bash_profile
      ```

   c. Add the STA bin directory to the `PATH` definition. For example, add the following line to the file:

      ```
      PATH=$PATH:<Oracle_storage_home>/StorageTek_Tape_Analytics/common/bin
      ```

      Where `Oracle_storage_home` is the Oracle storage home location specified during STA installation.
   d. Save and exit the file.
   e. Log out and log back in as the Oracle user.
   f. Confirm that the `PATH` variable has been updated correctly.

      ```
      $ echo $PATH
      /usr/lib64/qt-3.3/bin:/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/
      sbin:/sbin:/home/oracle/bin:/Oracle/StorageTek_Tape_Analytics/common/bin
      ```

2. Verify that all STA services are running and active:

   ```
   $ STA status all
   mysql is running
   staservd service is running
   staweblogic service is running
   staengine service is running
    .... and the deployed application for staengine is in an ACTIVE state
   staadapter service is running
    .... and the deployed application for staadapter is in an ACTIVE state
   staui service is running
    .... and the deployed application for staui is in an ACTIVE state
   ```

3. Proceed as follows:
   - If the STA services are running and active, you can begin configuring the libraries and STA. See Configure SNMP (for SL150, SL500, SL3000, SL8500).

- If there are any issues with the STA services, you can review the installation and STA logs for more information. See Logs Created During Installation, Upgrade, and Deinstallation for their locations.

Relocate the STA Logs Directory (optional)

Relocate the STA and MySQL logs to a location other than the default, which is `/var/log/tbi`.

After you complete this procedure, STA will write logs to the new location. You can perform this procedure anytime after STA has been installed. See Review the STA File System Layout for the location requirements.

1. On the STA server, open a terminal session. Log in as the system root user.
2. Stop all STA services:

   ```
   # STA stop all
   ```

3. Create the new logs directory. For example:

   ```
   # mkdir -p /LOGS_DIR/log/
   ```

4. Change access permissions to the directory so STA and MySQL can write to it. For example:

   ```
   # chmod 777 /LOGS_DIR/log
   ```

5. Move the current `/var/log/tbi` directory to the STA logs directory you have just created.

   ```
   # mv /var/log/tbi /LOGS_DIR/log
   ```

6. Create a symbolic link from your new STA logs directory to the default location. For example:

   ```
   # ln -s /LOGS_DIR/log/tbi /var/log/tbi
   ```

7. Restart STA:

   ```
   # STA start all
   ```

Register the Oracle Central Inventory Location

After STA installation, register the Oracle central inventory location on the STA server to create an Oracle central inventory pointer file, `/etc/oraInst.loc`.

The pointer file allows the Oracle central inventory location and Oracle group to be known to all Oracle installers used on the server.

1. On the STA server, open a terminal session. Log in as the Oracle user.
2. Display the location, as follows.
   - If the Oracle central inventory has been registered, you can display the contents of the `/etc/oraInst.loc` pointer file. The location is defined by the `inventory_loc` parameter, and the Oracle group is defined by the `inst_group` parameter.

     For example:

     ```
     $ cat /etc/oraInst.loc
     inventory_loc=/opt/oracle/oraInventory
     inst_group=oinstall
     ```

- If the Oracle central inventory has not been registered or the pointer file has been deleted, you can search for the Oracle central inventory, which has the directory name `oraInventory`. For example:

  ```
  $ find / -name oraInventory
  /opt/oracle/oraInventory
  ```

3. Change to the Oracle central inventory directory. You specify this directory the first time an Oracle product is installed on the STA server. For example:

   ```
   $ cd /opt/oracle/oraInventory
   ```

4. Switch to the root user. Run the registration script, located in that directory.

   ```
   # ./createCentralInventory.sh
   ```

   The Oracle central inventory location and the Oracle group and are now identified in the Oracle central inventory pointer file, `/etc/oraInst.loc`.

Logs Created During Installation, Upgrade, and Deinstallation

Use the STA installation, upgrade, and deinstallation logs to help troubleshoot issues.

Most log file names include a timestamp to help identify the installation or deinstallation instance. The timestamp is the date and time when the installation or deinstallation began.

In particular, the following logs provide valuable information if an installation, upgrade, or deinstallation fails.

- `installtimestamp.log`
- `sta_installtimestamp.log`
- `upgradetimestamp.log`
- `sta_upgradetimestamp.log`
- `deinstalltimestamp.log`
- `sta_deinstalltimestamp.log`

The locations of STA installation, upgrade, and deinstallation logs vary depending on the status of the operation. Logs are found in the following directories.

/tmp/OraInstall*timestamp*
This directory includes logs for in-progress installations, upgrades, and deinstallations. The logs are moved from this directory upon successful completion of the operation. Following is a sample listing of logs you might see in this directory during an operation.

```
install2016-09-24_04-14-04PM.log
installProfile2016-09-24_04-14-04PM.log
launcher2016-09-24_04-14-04PM.log
```

***/STA_home*/inventory/logs**
Where `STA_home` is the STA home location defined and created during STA installation (for example, `/Oracle/StorageTek_Tape_Analytics`).

This directory includes logs for installations, upgrades, and deinstallations that have completed successfully. Some logs, such as error or patch logs, are included only as applicable.
Following is a sample listing of logs you might see in this directory.

```
2016-08-05_01-55-59PM.log
install2016-08-05_01-55-59PM.log
install2016-08-05_01-55-59PM.out
installActions2016-08-05_01-55-59PM.log
OPatch2016-08-05_01-57-13-PM.log
OPatch2016-08-05_01-59-36-PM.log
oraInstall2016-08-05_01-55-59PM.err
oraInstall2016-08-05_01-55-59PM.out
```

***/STA_logs*/install**
By default, `STA_logs` is located at `/var/log/tbi`. You can optionally relocate this directory to a location of your choice any time after STA installation. See Relocate the STA Logs Directory (optional) for instructions.
This directory includes logs for installations, upgrades, and deinstallations that have completed successfully or failed. It includes logs related to the installation of the WebLogic server and MySQL database, as well as logs for installation and configuration of the STA application.
Following is a sample listing of logs you might see in this directory.

```
adf_install2016-08-05_01-55-51PM.log
dbinstall.log
dbinstall.mysqld.err
dbinstall.stadb-slow.log
install2016-08-05_01-42-09PM.log
patch_adf.log
sta_install2016-08-05_01-54-04PM.log
weblogic_install2016-08-05_01-55-34PM.log
```

Troubleshoot the Installation

If you have issues with installation, it may be an issue with SNMP, STA services, or the operating system configuration.

Refer to the following sections:

- Troubleshoot the Library Connection
- *STA Administration Guide* "Troubleshooting" appendix
  - Provides information on issues with accessing the GUI, exchanges not showing up, server processes not starting, or authentication prompts.

5

Configure Library Features for STA

Configure specific library features to ensure the library sends high-quality SNMP data to STA. Perform the applicable tasks on each library you want STA to monitor.

The SL500, SL3000, and SL8500 libraries have a command line interface (CLI) and a graphical user interface, the StorageTek Library Console (SLC). The SL150 and SL4000 libraries uses a browser-based user interface exclusively. You will use these interfaces to perform the procedures in this chapter. Refer to the product's *Library Guide* as needed.

- Log In to the Library
- Verify the Library Firmware Version
- Verify the HBT Drive Controller Card Version (SL3000 and SL8500 only)
- Enable ADI on the Library (SL500, SL3000, SL8500)
- Ensure the Correct Library Complex ID (SL8500 only)
- Set the Drive Cleaning Warning (optional, SL3000 and SL8500 only)
- Set Volume Label Format
- Set Element Addressing Mode (SL150 only)
- Disable the SCSI FastLoad Option (SL500 only)
- Avoid Duplicate Volume Serial Numbers
- Configure STA to Support Dual TCP/IP or RE (SL3000 and SL8500 Only)

Supporting Documentation:

The following tape storage documentation can be found at: https://docs.oracle.com/en/storage/tape-storage/index.html

- SL150 Library Guide
- SL3000 Library Guide
- SL4000 Library Guide
- SL8500 Library Guide

Log In to the Library

Log into the library CLI or user interface to configure the library features for STA.

Log into Library CLI (SL500, SL3000, and SL8500)

1. Review CLI Best Practices.
2. Establish an SSH connection to the library using the IP address or DNS alias.
3. Log in to the CLI using the `admin` username and password.

Log into SLC (SL500, SL3000, and SL8500)

1. Start the SLC application.
2. Click the **About** button to display the current SLC version and verify that it meets the library firmware minimum requirements.
3. Log in using the `admin` username, password, and library IP address or DNS alias.

   For SL3000 and SL8500 libraries with the Redundant Electronics feature, you can only log in to the active controller.

Log into the Browser Interface (SL150 and SL4000)

1. In a browser, go to the hostname or IP address of the library.
2. Log in with your user ID and password. The user must have the administrator role.

CLI Best Practices

Follow these best practices when using CLI commands.

For most CLI commands, the syntax is the same across the SL500, SL3000, and SL8500 library models. The details returned by each command may vary slightly from what is shown. Following are some tips for using the library CLI.

- Use a terminal emulator, such as PuTTY, to establish an SSH (secure shell) connection to the library CLI.
- Enable logging so you can review your activity to troubleshoot errors.
- With some firmware versions, the CLI times out after six hours.
- To display help for any CLI command, type `help` and the command name (for example, `help snmp`).
- SL500 commands are case-sensitive. SL3000 and SL85000 commands are not.
- Press the **Tab** key for automatic command completion.
- Press the **Up-Arrow** and **Down-Arrow** keys to scroll through your command history, then modify a previously entered command.

Use the Library Configuration Script for CLI Commands (optional)

STA provides a library configuration script to help complete the configuration. The script prompts for library configuration settings, and based on the values you enter, the script displays complete commands you can copy and paste into the library CLI.

1. Review and understand the library configuration steps in this chapter before initiating the script.
2. To initiate the script, open a terminal session on the STA server, log in as the Oracle user, and issue the following command:

   ```
   $ sh /<Oracle_storage_home>/StorageTek_Tape_Analytics/common/bin/STA-lib-config-steps.sh
   ```

   where `<Oracle_storage_home>` is the directory where STA and associated Oracle software are installed.

3. For additional information about the script and to see example usage, issue the following command:

   ```
   $ sh /<Oracle_storage_home>/StorageTek_Tape_Analytics/common/bin/STA-lib-config-steps.sh -? | more
   ```

Verify the Library Firmware Version

Verify that the library firmware meets or exceeds the minimum requirements. If it does not, submit a service request to Oracle Support to upgrade the firmware.

See Library Requirements for minimum firmware versions.

On the Library CLI (SL500, SL3000, and SL85000)

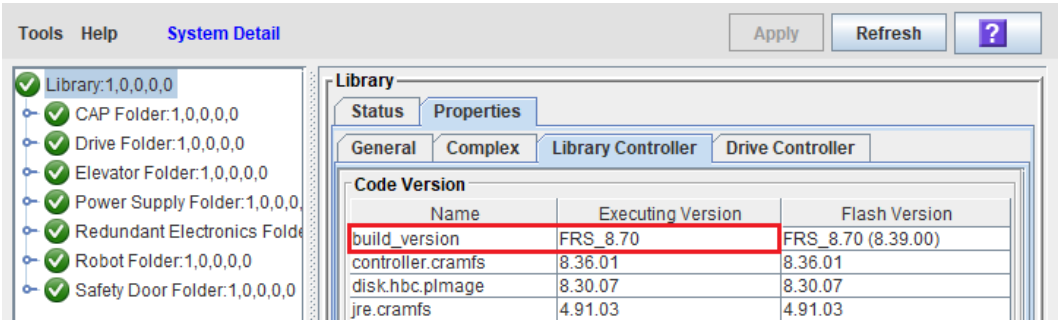
1. Execute the following command:

   ```
   version print
   ```

2. If the screen displays `SYNTAX ERROR!!`, the library firmware is down-level. Contact Oracle Support to upgrade the firmware

On SLC (SL500, SL3000, and SL85000)

1. In the **Tools** menu, select **System Detail**.
2. In the navigation tree, select **Library**.
3. Select the **Properties** tab, then select the **Library Controller** tab.



On the Browser Interface (SL150 and SL4000)

1. In the navigation tree, select **Firmware**.
2. The firmware version is displayed under the **Library Firmware** section. Alternately, you can click the **About** button in the status bar to obtain the firmware version.

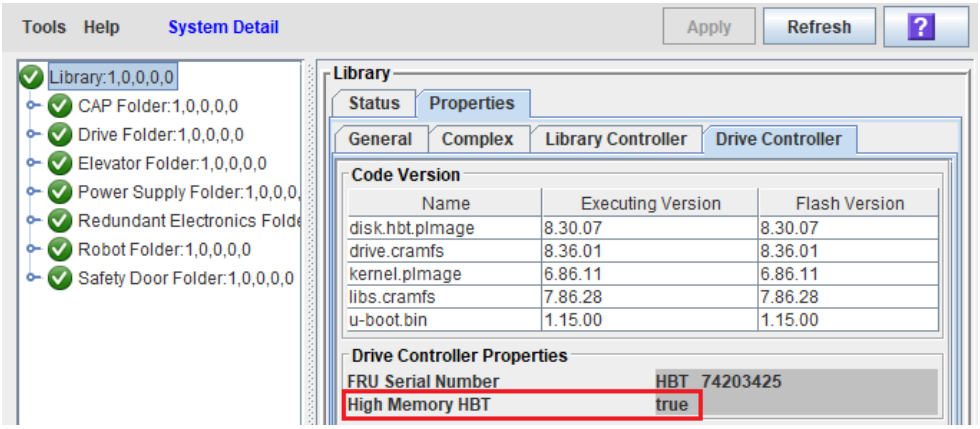
Verify the HBT Drive Controller Card Version (SL3000 and SL8500 only)

For SL3000 and SL8500 libraries to send rich drive data to STA, the library must have a high-memory drive controller (HBT) card. Verify that a high-memory HBT card is installed in the library.

See Library Requirements for HBT hardware requirements.

This procedure is performed using the SL Console. For SL8500 FRS 8.x and SL3000 FRS 4.x, you can also use the CLI `config print` command to display HBT information.

1. Using SLC, in the **Tools** menu, select **System Detail**.
2. In the navigation tree, select **Library**.
3. Select the **Properties** tab, then select the **Drive Controller** tab.
4. Verify that High Memory HBT indicates `true`.



5. If you have an SL3000 (FRS 4.x) or an SL8500 (FRS 8.x) library with Redundant Electronics, expand the Redundant Electronics folder, and then select each HBT card (hbta, hbtb). Both should indicate `True` for High Memory HBT.
6. If the library does not have a high-memory HBT card, submit a service request to Oracle Support to have one installed.

Enable ADI on the Library (SL500, SL3000, SL8500)

Ensure ADI is enabled on both the LTO drives and the library for STA tor receive rich drive data. By default ADI is disabled on the SL500, SL3000, and SL8500 libraries.

See also How the ADI Interface for LTO Drives Affects STA Data.

For SL3000 and SL8500 Libraries

1. Using the CLI, display the status of the ADI interface.

   ```
   drive adiEnable print
   ```

2. If "Attributes Adi Status" is `true`, quit this procedure.

   If it is `false`, enable the ADI interface:

   ```
   drive adiEnable on
   ```

3. Reboot the library to activate the change.

For SL500 Libraries

1. Using the CLI, display the status of the ADI interface.

   ```
   enableADI print
   ```

2. If "enableADI set to" is `on`, quit this procedure.

   If it is set to `off`, enable the ADI interface.

   ```
   enableADI on
   ```

3. Reboot the library to activate the change.

How the ADI Interface for LTO Drives Affects STA Data

LTO drives that support the Automation/Drive Interface (ADI) can provide rich data (for example drive performance and utilization) to the library, depending on drive configuration and firmware level.

For a library to send rich LTO drive data to STA, ADI must be enabled on both the library and the LTO drives. If ADI is not enabled on both, the library will only send basic data about the LTO drives. ADI is disabled by default on the SL500, SL3000, and SL8500 libraries.

See LTO Drive Requirements for details about required drive firmware levels.

Method for Enabling ADI on the Drives

The method for enabling ADI depends on the drive manufacturer and model.

- **HP LTO-3, 4, 5, and 6**: These drives switch automatically to ADI mode after ADI is enabled on the library, the library is rebooted, and the drives are rebooted. (Drives can be rebooted with SL Console.)
- **IBM LTO**: These drives must be explicitly configured for ADI mode and will not be recognized until ADI is enabled on the library and the library is rebooted. LTO-8 drives are shipped with ADI mode enabled by default. Verify the mode and set to ADI mode if necessary. The encryption adapter card provides the interface to the Oracle Key Manager (OKM) tape encryption solution. Both the drive and the encryption card firmware must meet the minimum requirements for STA.
  - **IBM LTO-3 and 4**: Oracle Support must configure the drive hardware to ADI.
  - **IBM LTO-5, 6, and 7 with the encryption card**: The drive firmware must be configured for ADI mode with Virtual Operator Panel (VOP). Contact Oracle Support for assistance.
  - **IBM LTO-8 and 9**: The drive firmware must be configured to ADI mode, if not already by default.

Enable ADI on the Library

By default, ADI is not enabled on SL500, SL3000, and SL8500 libraries, and you or Oracle Support must enable it manually. Because enabling ADI requires a reboot of the library, you should enable it in advance if you are planning to install LTO drives.

For SL3000 and SL8500 libraries, you can enable ADI only if the library has a high-memory drive controller (HBT) card. See Verify the HBT Drive Controller Card Version (SL3000 and SL8500 only).

Ensure the Correct Library Complex ID (SL8500 only)

Ensure each library complex at your site has a unique complex ID for STA to roll up library data correctly.

See also How the Library Complex ID Affects STA Data (SL8500 only).

> **Caution:**
>
> The Oracle Service Delivery Platform (SDP) also uses unique complex IDs for tracking library data. If your site uses SDP, contact Oracle Support before changing any complex ID. Changing the complex ID could cause SDP to fail. In most cases, complex IDs are set correctly when SDP is connected.

1. For each SL8500 library monitored by STA, use the CLI to display the complex ID currently assigned:

   ```
   SL8500> config complexId print
    ...
    Complex Id 3
    ...
   ```

2. Verify that each standalone library and each library complex has a unique complex ID, and that all libraries in each library complex share the same complex ID.

   If you need to change the complex ID of a *standalone* library, continue this procedure.

   > **Caution:**
   >
   > If you need to change the complex ID of a library in a *library complex*, contact Oracle Support. Do not continue with this procedure.

3. Place the library offline, and then wait for all transactions to complete.
4. Change the complex ID of a standalone library. `complex_ID` is a number, 1–127.

   config complexId set *complex_ID*

   For example:

   ```
   SL8500> config complexId set 5
    ...
    Complex Id 5
    Success true
    Done
    ...
    Note: TCP/IP stack reset may take a few seconds after command completion.
   ```

5. All TCP/IP connections are terminated when executing this command. You may have to log back in to the library.

How the Library Complex ID Affects STA Data (SL8500 only)

For STA to roll up library complex data correctly, each library complex at your site must have a unique complex ID.

On SL8500 libraries, complex IDs are set manually. On all other library models, the complex IDs are set automatically and therefore do not require manual intervention or verification.

Each standalone SL8500 is considered to be a separate complex and therefore must have a unique complex ID. In addition, each multi-library complex must have a unique complex ID, and all libraries within the complex must share the same ID. Valid complex ID values are 1–127.

Table 5-1 Example Complex ID Assignments

Complex Type	Libraries	Assigned Complex ID
Multi-library complex	SL8500-1 SL8500-2 SL8500-3	1 1 1
Standalone libraries	SL8500-4 SL8500-5	2 3

Set the Drive Cleaning Warning (optional, SL3000 and SL8500 only)

Check the current setting of the drive cleaning warning flag and change it if necessary.

If you have numerous drives in the library, you may want to set this flag to "off" so that the library top-level condition is not degraded whenever a drive needs cleaning.

See also How the Drive Clean Warning Affects STA Data (SL3000 and SL8500 only).

1. Using the CLI, display the current setting of the drive cleaning warning flag.

```
SL3000> cleaning driveWarning get
 ...
 Object Drive Cleaning Warning true
 ...
```

2. If you want to set the flag to `false` (off), use the following command:

```
cleaning driveWarning set off
```

How the Drive Clean Warning Affects STA Data (SL3000 and SL8500 only)

The drive cleaning warning flag indicates whether a drive warning should be issued whenever a drive needs cleaning. This flag is set at the library level, so the same setting applies to all drives in a library.

- When the flag is set to "on", each drive shows a warning health status whenever it needs cleaning. This also causes the top-level health status of the library to be degraded in the STA monitor and in SLC.
- When the flag is set to "off", each drive's status is not affected by the need for cleaning; therefore, the library top-level status in STA is not degraded.

Set Volume Label Format

All libraries must use the same volume label format.

> **Caution:**
>
> Incorrectly formatted volume serial numbers will block exchange processing, cause superfluous attempts to get data, and result in irreversible, eight-character volser records to appear on the Media – Overview screen. All libraries should use the default format "Trim last 2 characters". If using a non-default format, call service to determine if STA supports the configuration for your library type.

SL8500/SL3000

You do not need to configure anything for these library models.

SL4000

Select the "Trim Last Two Characters" volume label format when configuring the library settings or editing partition settings.

See the "Configure Library Settings" and "Edit a Partition" sections within the *SL4000 Library Guide* (https://docs.oracle.com/en/storage/tape-storage/sl4000/).

SL500

Set the host label orientation to `left6` and the `staConfig` flag to `on`. The STA config mode affects only how the SL500 sends the volser format to STA. It does not affect the format used by the SL500 library itself.

1. Stop all library activity.
2. Display the `orientlabel` flag.

```
SL500> orientlabel print
Host: (left8) Window left-justified with 6 character label
Op Panel: (left8) Window left-justified with 8 character label
```

3. Set the `host` flag to `left6`.

```
SL500> orientlabel host left6
```

4. Verify the new settings of the `orientlabel` flag.

```
SL500> orientlabel print
Host: (left6) Window left-justified with 6 character label
Op Panel: (left8) Window left-justified with 8 character label
```

5. Display the `staConfig` flag.

```
SL500> staConfig print
STA mode is disabled
```

6. Set the `staConfig` flag to `on`.

```
SL500> staConfig on
```

7. Verify the new settings of the `staConfig` flag.

```
SL500> staConfig print
STA mode is enabled
```

8. You may need to update the configuration of tape applications and hosts after changing these parameters.

SL150

Select the "Trim Last Two Characters" volume label format when configuring the library settings.

1. Stop all library activity.
2. In the browser interface, select **Configuration** in the navigation tree.
3. Click **Configure**  to launch the Configuration Wizard
4. Select the **Configure Library Settings** check box, and then click **Next**.
5. Set the following parameter, and then click **Next**.
   - **Library Volume Label Format** — Select *Trim last two characters (Default)*
6. On the Summary screen, select the **Accept all changes** check box, and then click **Apply**.
7. Select the **Set the Library back Online after applying the changes** check box, and then click **OK**.
8. When you see **All configuration changes have been applied successfully**, click **Close**.
9. You may need to update the configuration of tape applications and hosts after changing these parameters.

Set Element Addressing Mode (SL150 only)

Set the SL150 Drive Element Addressing Mode to "Address All Drive Slots" to include empty drive bays in the data sent to STA.

For SL150 firmware below 3.80, you must set the addressing mode to "Address All Drive Slots". However, version 3.80+ is compatible with STA in either addressing mode.

1. Stop all library activity.
2. In the browser interface, select **Configuration** in the navigation tree.
3. Click **Configure**  to launch the Configuration Wizard
4. Select the **Configure Library Settings** check box, and then click **Next**.
5. Set the following parameter, and then click **Next**.
   - **Drive Element Addressing Mode** — Select *Address All Drive Slots (Recommended)*
6. On the Summary screen, select the **Accept all changes** check box, and then click **Apply**.
7. Select the **Set the Library back Online after applying the changes** check box, and then click **OK**.

8. When you see **All configuration changes have been applied successfully**, click **Close**.
9. You may need to update the configuration of tape applications and hosts after changing these parameters.

   After changing the Drive Element Addressing Mode, you should wait at least 10 minutes before configuring SNMP in STA. If STA is already connected, wait 10 minutes, then initiate a manual MIB walk on the SL150 using the STA library connections screen. See Manually Collect Library Data. This will speed up any STA updates, otherwise it may take some time before the updated addresses are reflected within STA.

Disable the SCSI FastLoad Option (SL500 only)

The SCSI FastLoad option should be disabled on SL500 libraries, as cartridge mount traps are not properly sent to STA when SCSI FastLoad is enabled. FastLoad is disabled by default.

Contact Oracle Support if you are not sure of the status of this option.

Avoid Duplicate Volume Serial Numbers

In the STA data store, media history is retained by volume serial number (volser). Because all history for a particular piece of media is tied to its volser, Oracle recommends that you avoid duplicate volsers.

Volsers should be unique across all monitored libraries. Duplicate volsers will result in co-mingling of data for different pieces of media. See the *STA User's Guide* for additional detail about duplicate volsers.

Configure STA to Support Dual TCP/IP or RE (SL3000 and SL8500 Only)

STA is capable of maintaining uninterrupted connections with only up to two library IP addresses at a time. Therefore, on a given library, you can configure STA to support either Dual TCP/IP or Redundant Electronics (RE), but not both.

For libraries with both features, Oracle recommends that you configure STA to support Redundant Electronics, as this feature is more critical to maintaining continuous library operations.

If a library has both Redundant Electronics and Dual TCP/IP, the STA server's subnet must be different from the subnet of the library port not configured for STA (see Configure SNMP on the STA Server). Otherwise, the library may try to send data through those ports (unknown to STA), and the data will be rejected by STA. Make sure your default gateway is the 2B interface.

See the product's *Library Guide* for details about Dual TCP/IP and RE.

Table 5-2 Recommended Library IP Addresses for STA Connection

Activated Features	Primary Library IP	Secondary Library IP
Neither	2B port	NA
Dual TCP/IP only	2B port	2A port on the active card
Redundant Electronics only	2B port on the active card	2B port on the standby card
Both	2B port on the active card	2B port on the standby card

6

Configure the Library Connection (SNMP or SCI)

Depending on the library model, STA uses SNMP (SL150, SL500, SL3000, SL8500) or SCI (SL4000) to connect to the tape libraries in your system.

- Configure SNMP (for SL150, SL500, SL3000, SL8500)
- Configure SCI (for SL4000)
- Test the Library Connection
- Manually Collect Library Data
- Troubleshoot the Library Connection
- About the Monitored Libraries Table

Configure SNMP (for SL150, SL500, SL3000, SL8500)

STA uses Simple Network Management Protocol (SNMP) to monitor library activity for SL150, SL500, SL3000, and SL8500 models.

To configure SNMP, you must perform some configuration activities on the libraries and some on the STA server.

These procedures assume a basic understanding of SNMP and that you are using the recommended SNMP v3 protocol. The libraries send data to STA through SNMP traps and informs, and STA retrieves library configuration data through SNMP get functions. In SNMP terms, STA is a client agent and each library is a server agent.

Once the library and STA has an SNMP connection, STA generally receives data from the library continuously and without interruption. However, there are times when manual intervention is recommended or required to maintain or reestablish a connection.

> **Note:**
>
> Periodically, the MySQL Event Scheduler purges processed SNMP records from the database to minimize database growth.

- Configure SNMP on the Libraries
- Configure SNMP on the STA Server
- Update the SNMP Configuration After a Library or STA Change
- Troubleshoot the Library Connection
- Configure SNMP v2c Mode

Configure SNMP on the Libraries

Configure SNMP on the libraries to allow STA to receive SNMP traps. In SNMP terms, STA is a client agent and each library is a server agent.

To configure SNMP on the libraries, complete the following in the order listed:

- Retrieve the Library IP Address
- Enable SNMP on the Library
- Create an SNMP v3 User
- Retrieve the Library SNMP Engine ID (SL500, SL3000, SL8500)
- Create the STA SNMP v3 Trap Recipient
- Create the STA SNMP v2c Trap Recipient

Retrieve the Library IP Address

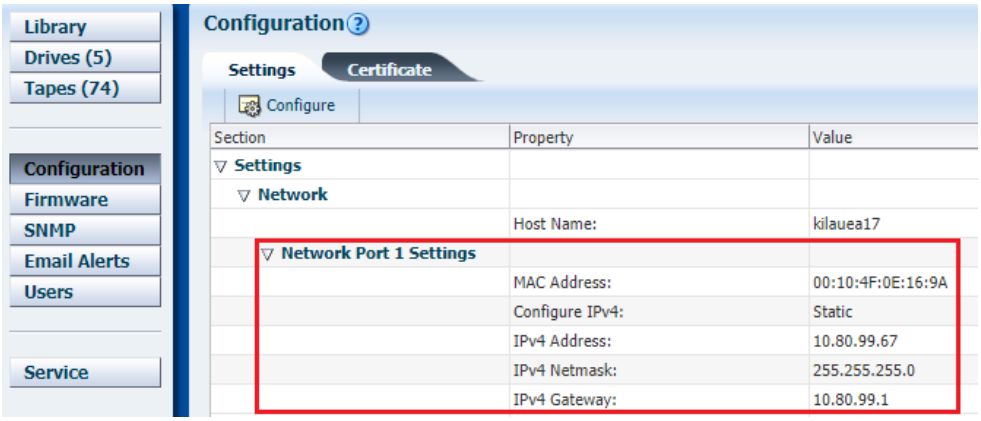
Retrieve and record the library IP address so that you can configure the STA connection with the library.

For SL3000 and SL8500 libraries, choose the method that corresponds to the library's configuration, either: Redundant Electronics, Dual TCP/IP, or neither.

SL150

1. In the browser interface, select **Configuration** in the navigation tree.
2. Within the Network section, the library IP address is displayed in the **Network Port 1 Settings** (the Network Port 2 is reserved for service use).

> **Note:**
>
> The address must be `Static`. If it is not, click **Configure**  , and then select **Configure Network Settings** to specify a static IP address.

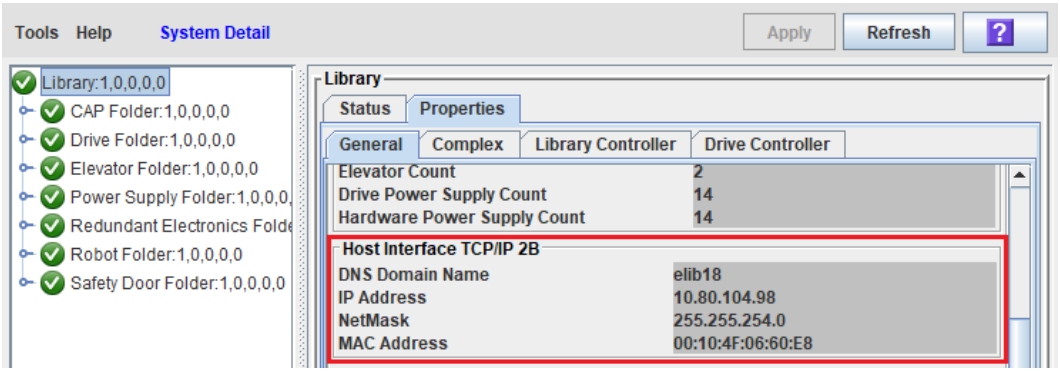


SL500

1. Using SLC, from the **Tools** menu, select **System Detail**.
2. In the navigation tree, select **Library**.
3. Select the **Properties** tab, then select the **General** tab.
   The library IP address is listed under the Library Interface TCP/IP section.
4. Record the library IP address as the primary library IP address. (This address corresponds to the 1B port.)

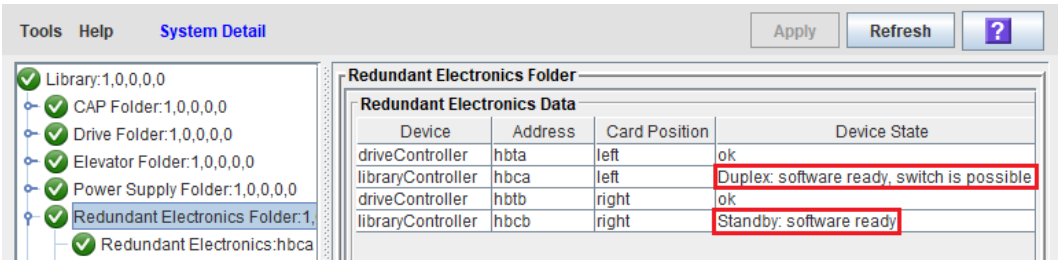
SL3000 or SL8500 - Neither Dual TCP/IP nor RE

1. Using SLC, from the **Tools** menu, select **System Detail**.
2. In the navigation tree, select **Library**.
3. Select the **Properties** tab and **General** sub-tab.
4. The IP address information is displayed in the Host Interface TCP/IP 2B section. There is no IP address information in the 2A section.
   Record the IP address as the primary library IP address.



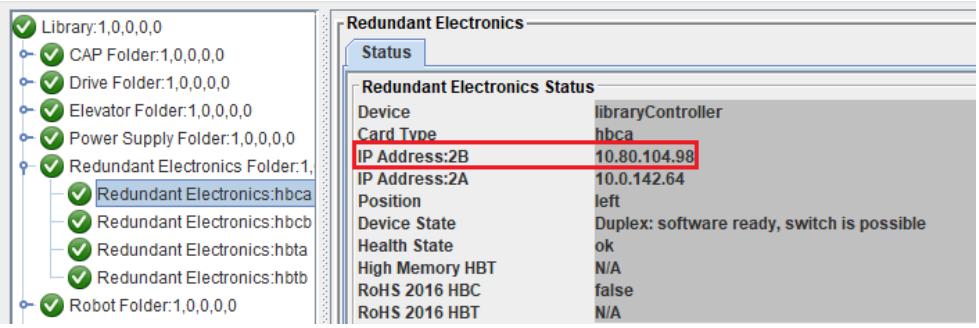
SL3000 or SL8500 - Redundant Electronics Support

1. Using SLC, from the **Tools** menu, select **System Detail**.
2. In the navigation tree, select the **Redundant Electronics** folder.
   If this folder is not listed, the Redundant Electronics is not available on the library.
3. In the Device State field, verify that one library controller shows `Duplex: software ready, switch possible` (this is the active card) and the other shows `Standby: software ready` (this is the standby card).



These statuses indicate that the controller cards are functioning normally. If you do not see these statuses, contact Oracle Support.

4. Expand the **Redundant Electronics** folder, and then select the active controller card. Record the IP address of the 2B port.



5. Repeat for the alternate (standby) controller card.

SL3000 or SL8500 - Dual TCP/IP Support

1. Using SLC, from the **Tools** menu, select **System Detail**.
2. In the navigation tree, select **Library**.
3. Select the **Properties** tab, then select the **General** tab.

   The IP address information is displayed in the Host Interface TCP/IP 2B and Host Interface TCP/IP 2A sections.

> **Note:**
>
> If the library also includes the Redundant Electronics feature, the IP addresses displayed are for the active controller card only.

4. Record the primary IP address (2B section) and secondary IP address (2A section).

Enable SNMP on the Library

Enable SNMP on the library public port so that the library can send data to STA.

SL3000 and SL8500

Enable SNMP on port 2B using the CLI. If the library includes the Dual TCP/IP feature, this command also enables SNMP on port 2A.

```
> snmp enable port2b
```

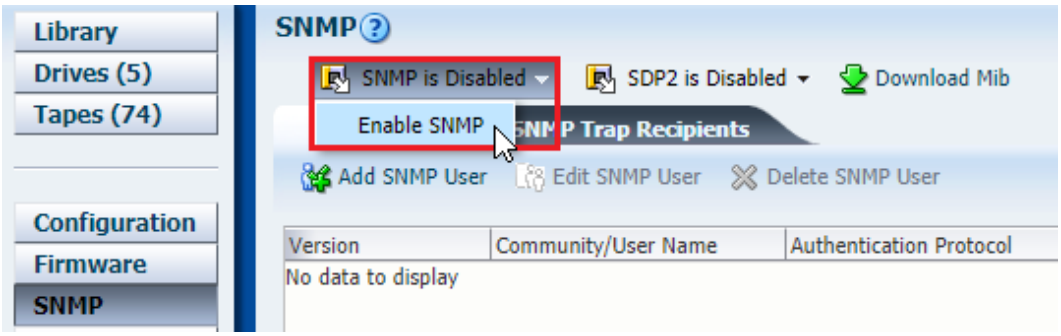
SL500

Enable SNMP on port 1B using the CLI.

```
> snmp enable port1B
```

SL150

1. In the browser interface, select **SNMP** in the navigation tree.
2. If SNMP shows as disabled, select **Enable SNMP**.



Create an SNMP v3 User

The SNMP v3 user sends SNMP traps and MIB (management information base) data to the STA server.

Requirements

- The authorization method must be `SHA` (Secure Hash Algorithm), and the privacy method must be `DES` (Data Encryption Standard).
- All SNMP libraries must use the same SNMP v3 credentials. Define a unique SNMP v3 user for this purpose and then define this same user on all monitored libraries.
- Do no *not* use the values "public" or "private" for the SNMP v3 username, as these values are well known and present a security risk. Use values that are not as easily discovered. The username can only contain alphanumeric characters (a–z, A–Z, 0–9). Special characters are not allowed.
- Authorization and privacy passwords must be at least eight characters in length, and cannot contain commas, semicolons, or equal signs.

SL500, SL3000, and SL8500

> **Note:**
>
> All SNMP libraries must use the same SNMP connection credentials. Define the same username and passwords on all SNMP libraries that will be monitored by this instance of STA.

1. Using CLI, create an SNMP v3 user:

   ```
   > snmp addUser version v3 name name auth SHA authPass auth_password priv DES
   privPass priv_password
   ```

   Where:

- `name` is the SNMP v3 username
- `auth_password` and `priv_password` are the authorization password and privacy password.

For SL3000 and SL8500 libraries, enclose variables in single quotes. For example:

```
SL3000> snmp addUser version v3 name 'STAsnmp' auth SHA authPass 'authpwd1'
priv DES privPass 'privpwd1'
```

For SL500, do not use quotes. For example:

```
SL500> snmp addUser version v3 name STAsnmp auth SHA authPass authpwd1 priv
DES privPass privpwd1
```

2. List the SNMP users to verify that the SNMP v3 user has been added correctly.

```
> snmp listUsers
```

SL150

> **Note:**
>
> All SNMP libraries must use the same SNMP connection credentials. Define the same username and passwords on all SNMP libraries that will be monitored by this instance of STA.

1. In the browser interface, select **SNMP** in the navigation tree.
2. In the SNMP Users section, select **Add SNMP User**  .
3. For Version, select `v3`, and then complete the information as follows:
   - **User Name**: The name of the SNMP v3 user.
   - **Authentication Protocol**: Select `SHA`.
   - **Authentication Passphrase**: Specify an authorization password.
   - **Privacy Protocol**: Select `DES`.
   - **Privacy Passphrase**: Specify a privacy password.

Retrieve the Library SNMP Engine ID (SL500, SL3000, SL8500)

Display the library's SNMP engine ID to use when you define STA as the SNMP v3 trap recipient. In the case of SL8500 library complexes, each library in the complex has its own SNMP agent, and therefore its own unique engine ID.

1. Using the CLI, use one of the following commands:
   - For SL3000 and SL8500 libraries:

     ```
     > snmp engineId print
     ```

   - For SL500 libraries:

     ```
     > snmp engineId
     ```

2. Save the engine ID (for example, 0x81031f88804b7e542f49701753) to a text file for use in the remaining SNMP configuration tasks.

Create the STA SNMP v3 Trap Recipient

Define the STA server as an authorized recipient of SNMP v3 traps. Define the traps that the library will send.

Note the following configuration requirements:

- To avoid duplicate records, do not define the STA server as a trap recipient in multiple instances. For example, do not create both an SNMP v3 and SNMP v2c trap recipient definition for the STA server.
- Trap levels 13 (Test Trap) and 14 (Health Trap) were added in STA 2.0.x. Trap level 4 may not be supported by older library firmware versions; however, it can always be specified when creating a trap recipient.

SL500, SL3000, SL8500

1. Create an SNMP v3 trap recipient. Separate the trap levels with commas.

   ```
   > snmp addTrapRecipient trapLevel
   1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host STA_server_IP version v3
   name recipient_name auth SHA authPass auth_password priv DES privPass
   priv_password engineId library_engineID
   ```

   Where:

   - `STA_server_IP` is the IP address of the STA server.
   - `recipient_name` is the SNMP username you created in for the SNMPv3 user.
   - `auth_password` and `priv_password` are the authorization and privacy passwords you created in for the SNMPv3 user.
   - `library_engineID` is the library engine ID you displayed in Retrieve the Library SNMP Engine ID (SL500, SL3000, SL8500), including the 0x prefix.

   For SL3000 and SL8500 libraries, enclose `recipient_name`, `auth_password`, and `priv_password` in single quotes. For example:

   ```
   SL3000> snmp addTrapRecipient trapLevel
   1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host 192.0.2.20 version v3 name
   'STAsnmp' auth SHA authPass 'authpwd1' priv DES privPass 'privpwd1' engineId
   0x00abcdef000000000000000000
   ```

   For SL500, do not use quotes. For example:

   ```
   SL500> snmp addTrapRecipient trapLevel
   1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host 192.0.2.20 version v3 name
   STAsnmp auth SHA authPass authpwd1 priv DES privPass privpwd1 engineId
   0x00abcdef000000000000000000
   ```

2. List the trap recipients, and verify the recipient has been added correctly.

   ```
   > snmp listTrapRecipients
   ```

SL150

1. In the browser interface, select **SNMP** in the navigation tree.
2. In the SNMP Trap Recipients section, select **Add Trap Recipient** .
3. Complete the fields as follows:

- **Host Address**—IP address of the STA server.
- **Trap Level**—Comma-separated list of trap levels the library should send to STA: 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100.
- **Version**—Select `v3`.
- **Trap User Name**—SNMP username you created for the SNMPv3 user.
- **Authentication Protocol**—Select `SHA`.
- **Authentication Passphrase**—Authorization password you created for the SNMPv3 user.
- **Privacy Protocol**—Select `DES`.
- **Privacy Passphrase**—Privacy password you created for the SNMPv3 user.
- **Engine ID**—This field will be supplied automatically. Do not modify the value.

Configure SNMP on the STA Server

After configuring SNMP on the libraries, configure SNMP on the STA server.

To configure SNMP on the STA server, complete the following in the order listed:

- Sign In to the STA GUI
- Verify SNMP Communication with a Library (optional)
- Configure SNMP Client Attributes for STA
- Configure the SNMP Connection to a Library
- Test the Library Connection
- Manually Collect Library Data

Sign In to the STA GUI

Most SNMP configuration will take place using the browser interface. Log in to the GUI as an administrator user.

1. Go to: **`http(s)://`**`<host_name>:<port>`**`/STA/`**

   Where:

   - `<host_name>` is the hostname of the STA server.
   - `<port>` is the STA port number you specified during installation. The default HTTP port is 7021. The default HTTPS port is 7022.
   - `STA` must be uppercase.

   For example: `https://staserver.example.com:7022/STA/`

2. Enter the STA administrator username and password.

   The first time you sign in after installation, it may take up to 30 seconds to authenticate the user and display the STA screens. This is normal, and future logins should occur without this delay.

Verify SNMP Communication with a Library (optional)

Confirm the SNMP connection between the STA server and each library it monitors.

This procedure verifies that UDP ports 161 and 162 have been enabled on all network nodes between the STA server and the library. It cannot validate that an SNMP v3 trap recipient has been specified correctly.

1. Perform this procedure for each monitored library. For each SL3000 or SL8500 library with either RE or Dual TCP/IP, perform this procedure twice: once for the primary library IP address and once for the secondary IP address.
2. On the STA server, open a terminal window. Log in as the Oracle user.
3. Test the SNMP v3 connection. The values you specify must match the corresponding ones on the library.

   ```
   $ snmpget -v3 -u <SNMP v3 username> -a SHA -A <authorization password> -x DES -X
   <privacy password> -l authPriv <library_IP_addr> 1.3.6.1.4.1.1211.1.15.3.1.0
   ```

   Where:

   - `<library_IP_addr>` is the IP address of the public port on the library.
     - For SL150 libraries, this is Network Port 1.
     - For SL500 libraries, this is port 1B.
     - For SL3000 and SL8500 libraries, there may be multiple ports to test, depending on whether Dual TCP/IP or Redundant Electronics are activated on the library. If there are multiple ports, run this command for each IP address.
   - **`1.3.6.1.4.1.1211.1.15.3.1.0`** is the SNMP object identifier (OID) for the library, which is the same for all library models.

   If the command output displays the library model, the test is successful. Following are some command examples.

   Successful snmpget command:

   ```
   $ snmpget -v3 -u STAsnmp -a SHA -A authpwd1 -x DES -X privpwd1 -l
   authPriv 192.0.2.20 1.3.6.1.4.1.1211.1.15.3.1.0
   SNMPv2-SMI::enterprises.1211.1.15.3.1.0 =STRING: "SL8500"
   ```

   Failed snmpget commands:

   ```
   $ snmpget -v3 -u STAsnmp -a SHA -A authpwd1 -x DES -X privpwd1 -l authPriv
   192.0.2.20 1.3.6.1.4.1.1211.1.15.3.1.0
   Timeout: No Response from 192.0.2.20.

   $ snmpget -v3 -u WrongUsr -a SHA -A authpwd1 -x DES -X WrongPwd -l authPriv
   192.0.2.20 1.3.6.1.4.1.1211.1.15.3.1.0
   snmpget: Authentication failure (incorrect password, community or key)
   ```

4. Test the SNMP v2c connection.

   ```
   $ snmpget -v2c -c stasnmp -l authPriv <IP address of library public port>
   ```

5. If both SNMP connection tests are successful, quit this procedure.

   If either test fails, proceed to the next step to troubleshoot suspected network issues, as necessary.

6. Use these steps only if the SNMP connection test are not successful. These steps require system root permissions.

   a. Log in as the system root user.

      ```
      $ su root
      ```

   b. Confirm packet routing from the STA server to the library.

      ```
      # traceroute -I <IP address of library public port>
      ```

      The output shows the number of hops and the round-trip time to reach each one. The round-trip time (the last line in the command output) should be less than one second. If it is not, confirm the network's performance with your network administrator.

   c. Monitor TCP/IP packets sent between the STA server and the library.

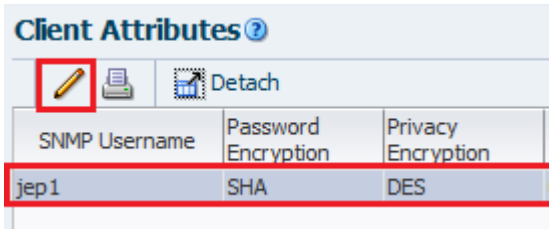
      ```
      # tcpdump -v host <IP address of library public port> > /var/tmp/<file name of output> &
      ```

Configure SNMP Client Attributes for STA

Add or modify SNMP client settings for STA. These settings configure STA to receive SNMP data from one or more libraries. A single SNMP client entry is used to connect to all SNMP libraries monitored by STA.

1. In the STA GUI, expand the **Setup & Administration** tab, and then select **Library Connections**.

2. Select the row in the Client Attributes table, and then click **Edit** .



3. Complete all fields in the dialog. The values you specify must match the corresponding values used on the libraries. Even if STA will only be monitoring libraries configured for SNMP v2c communication, you must complete all fields, including those applicable to SNMP v3. You cannot leave any fields blank.

> **Note:**
>
> All SNMP libraries must use the same SNMP connection credentials. The username and passwords entered will apply to all SNMP libraries monitored by this instance of STA.

- **STA SNMP Connection Username (Auth)**—Type the SNMP v3 username.
- **Enter STA SNMP Connection Password (Auth)**—Type the connection authorization password.

- **Enter Privacy Encryption Password (Privacy)**—Type the privacy encryption password.
- **User Community**—Type the SNMP v2c community string specified on the library. This field is required for the SNMP handshake with the library.
- **Trap Community** —Type the SNMP v2c community string specified on the library. This field is used only if SNMP v2c is used for communication with the library.

4. Click **Save**.
5. Click **OK** to dismiss the message. You will perform the connection test later.

Configure the SNMP Connection to a Library

Add each SL150, SL500, SL3000, and SL8500 library you want STA to monitor to the Monitored Libraries table.

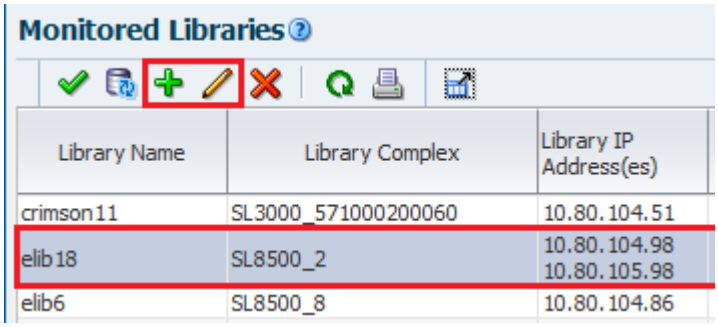
For existing connections, you must complete this procedure if there are changes to any of the SNMP configuration settings on a monitored library, such as a change to the library IP address.

If you are configuring multiple library connections at one time, to minimize library disruption, complete this procedure for all libraries before testing the SNMP connections.

1. In the STA GUI, expand the **Setup & Administration** tab, and then select **Library Connections**.
2. In the Monitored Libraries table:

   To configure a connection for the first time, click **Add** .

   To modify an existing connection, select a library in the table, then click **Edit** .



3. Select **SNMP** for the connection type.
4. Complete the dialog box. The values you specify must match the corresponding ones on the library.
   - **Library Name**—A name to identify the library throughout the STA user interface screens (for example, the library host name).
   - **Library Primary IP Address**—The IP address of the primary public port on the library.
   - **Library Secondary IP Address**—Applies only to libraries using dual TCP/IP or redundant electronics (RE). Specify the IP address of the secondary public port on the library. Leave the field blank for libraries that do not have dual TCP/IP or RE.

- **STA IP Address**—Select the IP address of the STA server.
- **Library Engine ID**—Do not change this field. This is the unique SNMP engine ID of the library, and it is automatically provided when the initial connection between STA and the library is made. It is blank for new connections.
- **Automated Daily Data Refresh**—Specify the time of day you want STA to collect the latest configuration data from the library. The data is collected automatically every 24 hours at this time. You should choose a time when there is typically lighter library usage. The default is 00:00 (12:00 am). Use 24-hour time format.

> **Caution:**
>
> If you leave this field blank, scheduled automatic library data collections are disabled. This will cause your STA library configuration data to become out of sync with the library.

- **Library Time Zone**—Select the library's local time zone.

5. Click **Save**. Click **OK** to dismiss the Library Connection Test message. You will perform the test after adding all libraries.
6. Repeat for each library monitored by STA.
7. After adding all the libraries, proceed to Test the Library Connection.

Update the SNMP Configuration After a Library or STA Change

To maintain communication between STA and the libraries, you must update the SNMP configuration after making any changes to the configuration.

- Update SNMP After a Redundant Electronics Switch (SL3000, SL8500)
- Update SNMP After a Library Firmware Upgrade (SL500, SL3000, SL8500)
- Update SNMP After Changing the STA Server IP Address
- Remove a Library Connection from STA
- Delete or Modify the STA Trap Recipient

Update SNMP After a Redundant Electronics Switch (SL3000, SL8500)

If STA is configured to support Redundant Electronics (RE) and a controller card switch occurs, STA maintains a connection with the library through the port specified as the secondary library IP address. However, you must also perform a manual procedure after the switch completes.

1. Wait 15 minutes after the newly active controller card has fully initialized.
2. Perform a connection test to verify the library SNMP connection. See Test the Library Connection.
3. Perform a data collection to retrieve the current library configuration data. See Manually Collect Library Data.

4. If a controller card is replaced after the RE switch, the IP address for the library changes, so you must reenter the SNMP connection information in STA. See Configure the SNMP Connection to a Library.

Update SNMP After a Library Firmware Upgrade (SL500, SL3000, SL8500)

Update the library and STA SNMP configurations after upgrading to one of the following library firmware versions or higher. Starting with these firmware versions, the library engine ID uses a new 32-bit value and therefore you must update the SNMP configuration to use the new ID.

- SL500 – FRS 1468
- SL3000 – FRS 4.0
- SL8500 – FRS 8.0

Update the SNMP Settings in STA

1. Log in to the STA user interface.
2. Edit the library connection details for the upgraded library. See Configure the SNMP Connection to a Library.

   In the Define Library Connection Details dialog box, clear the Library Engine ID field and click **Save**. This forces STA to update the engine ID to the new value when it reconnects to the library.
3. Re-establish the SNMP connection with the library. See Test the Library Connection.
4. Record the new SNMP engine ID displayed on the SNMP connections table. You will use this value in the next part of the procedure.

Verify SNMP Settings on the Library

1. Log in to the CLI on the upgraded library.
2. Display All SNMP Trap Recipients.
3. Verify the SNMP Version level for the STA server, and proceed as follows:
   - If it is `v2c`, you can quit this procedure.
   - If it is `v3`, continue to the next step.
4. Compare the displayed engine ID with the one you noted in the first part of this procedure:
   - If they match, you can quit this procedure.
   - If they do not match, continue to the next step.
5. Record the Index number of the STA trap recipient.
6. Delete the STA trap recipient. See Delete or Modify the STA Trap Recipient.
7. Re-add the STA SNMP v3 trap recipient using the new library engine ID. See Create the STA SNMP v3 Trap Recipient.

Update SNMP After Changing the STA Server IP Address

If the IP address of the STA server has been changed, use this procedure to ensure SNMP connectivity between STA and all monitored libraries. You must perform the complete procedure for each monitored library.

Confirm Network and SNMP Connectivity

Confirm good communication between STA and the library. See Verify SNMP Communication with a Library (optional) for instructions.

Update SNMP Settings on the Library

1. Retrieve the index number of the STA trap recipient. See Display All SNMP Trap Recipients for instructions.
2. Delete the STA trap recipient with the old IP address. See Delete or Modify the STA Trap Recipient for instructions.
3. Add the STA trap recipient with the new IP address. See Create the STA SNMP v3 Trap Recipient.

Update SNMP Settings in STA

1. Update the STA IP address in the SNMP connection settings. See Configure the SNMP Connection to a Library for instructions.
2. Reestablish the SNMP connection with the library. See Test the Library Connection for instructions.
3. Update the library configuration data. This step is necessary only if drive or media configuration changes have occurred on the library. See Manually Collect Library Data for instructions.

Remove a Library Connection from STA

A disconnected library will no longer send data to STA. All existing data for the library will be removed from the STA screens but will be retained in the STA database.

1. In the left navigation, expand **Setup & Administration**, then select **Library Connections**.
2. In the Monitored Libraries table, select the library, and then click **Delete**  .
3. For SNMP connections, you must also delete the STA SNMP trap recipient from the library. See Delete or Modify the STA Trap Recipient.

Delete or Modify the STA Trap Recipient

Change or delete the STA trap recipient on the library. For all library models except SL150, to modify a trap recipient definition, you must first delete the existing definition and then add a new one.

SL150

1. Log in to the browser-based user interface.
2. In the navigation tree, select **SNMP**, then select **SNMP Trap Recipients**.

3. Select a trap recipient from the list.
4. Select **Edit Trap Recipient** or **Delete Trap Recipient**.
5. If modifying a trap recipient, modify the settings, and then click **Save**.

SL500, SL3000, and SL8500

1. Log in to the library CLI.
2. Delete the trap recipient.

   snmp deleteTrapRecipient id *index*

   Where `index` is the index number of the trap recipient to be deleted.

   For example: `ADMIN> snmp deleteTrapRecipient id 1`
3. Re-add the trap recipient, as necessary (see Create the STA SNMP v3 Trap Recipient).

Configure SNMP v2c Mode

STA only supports v2c mode to provide compatibility with legacy systems. Oracle does not recommend using v2c. Instead, use v3 for maximum security.

To configure the libraries and STA to use SNMP v2c:

1. Follow all procedures in Configure SNMP on the Libraries, except:
   - Replace Create an SNMP v3 User with Create an SNMP v2c User.
   - Replace Create the STA SNMP v3 Trap Recipient with Create the STA SNMP v2c Trap Recipient.
   - After completing all procedures in Configure SNMP on the Libraries, complete Enable SNMP v2c Mode for STA
2. Configure SNMP v2c on the STA server, see Configure SNMP on the STA Server.

When to Use v2c Mode

Only use v2c if a legacy system requires it. To use the media validation feature and to maximize security, you must use the SNMP v3 protocol.

The SNMP v2c protocol is less secure than SNMP v3. By default, STA does not have v2c enabled. However, if your legacy systems do not support SNMP v3 communication, you can enable and configure SNMP v2c mode for STA.

Create an SNMP v2c User

If you are using SNMP v2c, define a community string.

Requirements

- STA supports only one SNMP v2c community string. You should define a unique community string for this purpose, and then define this same community string on all libraries monitored by that STA instance.
- Do *not* use the values "public" or "private" for the STA community string, as these values are well known and present a security risk. Use values that are not easily discoverable.

The community string can only contain alphanumeric characters (a–z, A–Z, 0–9). Special characters are not allowed.

- If a library includes a community string set to "public", do not remove it without first consulting Oracle Support. In some cases, a community string with this value is required for Oracle Service Delivery Platform (SDP).

SL500, SL3000, and SL8500

1. Using CLI, add the SNMP v2c user.

   ```
   > snmp addUser version v2c community community_name
   ```

   Where `community_name` is the SNMP v2c user community string. For example:

   ```
   SL3000> snmp addUser version v2c community stasnmp
   ```

2. List the SNMP users to verify that the SNMP v2c user has been added correctly.

   ```
   > snmp listUsers
   ```

SL150

1. In the browser interface, select **SNMP** in the navigation tree.
2. Click **Add SNMP User**  .
3. Complete the Add SNMP User screen as follows:
   - `Version`: Select `v2c`.
   - `Community Name`: Specify the SNMP v2c user community string (for example, `stasnmp`).

Create the STA SNMP v2c Trap Recipient

If you are using SNMP v2c, define the STA server as an authorized recipient of SNMP v2c traps and to define traps the library sends.

Note the following configuration requirements:

- To avoid duplicate records, do not define the STA server as a trap recipient in multiple instances. For example, do not create both an SNMP v3 and SNMP v2c trap recipient definition for the STA server.
- Trap level 4 may not be supported by older library firmware versions; however, it can always be specified when creating a trap recipient.
- To avoid entry errors in the CLI, you can first type the command in a text file, and then copy and paste it into the CLI. For help with CLI commands, type `help snmp`.
- Do *not* use the values "public" or "private" for the community string, as these values are well known and present a security risk.

SL500, SL3000, and SL8500

1. Establish a CLI session on the library.
2. Create an SNMP v2c trap recipient. Separate trap levels with commas.

   ```
   > snmp addTrapRecipient trapLevel 1,2,3,4,11,13,14,21,25,27,41,45,
   61,63,65,81,85,100 host STA_server_IP version v2c community community_name
   ```

Where:

- `STA_server_IP`: IP address of the STA server.
- `community_name`: SNMP v2c trap community string.

For example:

```
> snmp addTrapRecipient trapLevel
1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host 192.0.2.20 version v2c
community stasnmp
```

3. List the trap recipients to verify that STA has been added correctly.

```
> snmp listTrapRecipients
...
Trap Level 1,2,3,4,11,13,14,21,25,27,41,45, 61,63,65,81,85,100
Version v2c
Object Snmp snmp
```

SL150

1. Log in to the library.
2. In the navigation tree, select **Settings**.
3. Select the **SNMP** tab.
4. In the SNMP Trap Recipients table, select **Add Trap Recipient**.
5. Complete the Add Trap Recipient screen as follows:
   - **Host Address** - IP address of the STA server.
   - **Trap Level** - Comma-separated list of trap levels the library should send to STA: 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
   - **Version** - Select `v2c`.
   - **Community Name** - Specify the SNMP v2c trap community string (for example, `stasnmp`).
6. Click **OK** to add the trap recipient.

Enable SNMP v2c Mode for STA

If using SNMP v2c, you must first enable it on the STA server. By default, SNMP v2c is disabled.

1. Do not perform this procedure if you are using SNMP v3.
2. Establish a terminal session with the STA server and log in as the Oracle user.
3. Change to the STA configuration files directory.

```
$ cd /Oracle_storage_home/Middleware/user_projects/domains/TBI
```

Where `Oracle_storage_home` is the Oracle storage home location defined during STA installation.

4. Edit the SNMP version properties file.

```
$ vi TbiSnmpVersionSupport.properties
```

5. Change the SNMP v2c parameter to `true`.

```
V2c=true
```

6. Save and exit the file.
7. Stop and restart all STA processes to activate the change.

```
$ STA stop all
$ STA start all
```

Configure SCI (for SL4000)

The SL4000 library uses the StorageTek Control Interface (SCI) to communicate with STA.

STA will automatically configure both SCI and outbound SCI (OSCI) connections once you add the SL4000 to the list of Monitored Libraries. You must provide the correct SL4000 library IP address and credential information.

Add the SL4000 as a Monitored Library

STA will automatically configure both SCI and outbound SCI (OSCI) connections once you add the SL4000 to the list of Monitored Libraries. You must provide the correct SL4000 library IP address and credential information.

Prerequisites before connecting STA to an SL4000

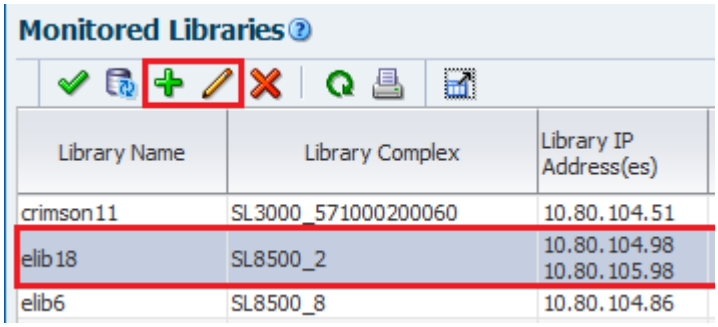
- Obtain the credential information for an SL4000 user with the "User" role to be used by STA to communicate using SCI.
- Obtain the credential information for an STA account to be used by the SL4000 to communicate to STA using outbound SCI.
- Configure the STA server firewall settings for the following:
  - To allow HTTP/HTTPS outbound connections to the SL4000 IP address and port (default is 7102 for HTTP and 7103 for HTTPS)
  - To allow HTTPS inbound connections from the SL4000 IP address and port (default is 7026)
- Configure all network routers, proxy servers, and firewalls to allow for inbound and outbound SCI traffic between the library and STA server.

Procedures

1. Before proceeding, ensure that you have completed all prerequisites listed above.
2. In the STA GUI, expand the **Setup & Administration** tab, and then select **Library Connections**.
3. In the Monitored Libraries table:

   To configure a connection for the first time, click **Add**  .

   To modify an existing connection, select a library in the table, then click **Edit**  .



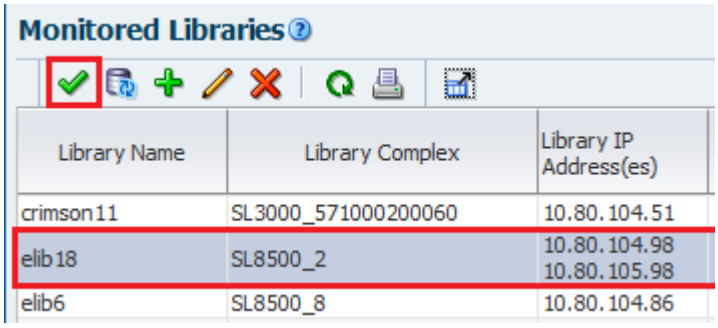
4. Select **Library API** for the connection type.
5. Complete the dialog box:
   - **Library Name**—A name to identify the library throughout the STA user interface screens (for example, the library host name).
   - **Library Primary IP Address**—The IP address of the primary public port on the library.
   - **Library Secondary IP Address**—Applies only to libraries using dual TCP/IP or redundant electronics (RE). Specify the IP address of the secondary public port on the library. Leave the field blank for libraries that do not have dual TCP/IP or RE.
   - **STA IP Address**—Select the IP address of the STA server.
   - **STA-to-Library User ID**—User ID for the SL4000 user account to be used by STA for SCI communication. The account must have the "User" role. See the SL4000 documentation for how to create a user account.
   - **STA-to-Library Password**—Password of the SL4000 user account.
   - **Library-to-STA User ID**—User ID for the STA account to be used by the library for OSCI communication.
   - **Library-to-STA Password**— The password for the STA account.
   - **Library HTTP port**— The port used for SCI HTTP communications. The default is 7102.
   - **Library HTTPS port**— The port used for SCI HTTPS communications. The default is 7103.
   - **Automated Daily Data Refresh**—The time of day you want STA to collect the latest library configuration data. STA automatically collects the data every 24 hours at this time. Choose a time when there is typically lighter library usage. The default is 00:00 (12:00 am). Use 24-hour time format.
   - **Library Time Zone**—Select the library's local time zone.
6. Click **Save**.
7. Repeat for each SL4000 library monitored by STA.
8. After adding all the libraries to the Monitored Libraries table, you should test the connection to each library. Proceed to Test the Library Connection.
9. If you want to skip the test, proceed to Manually Collect Library Data.

Test the Library Connection

Test the connection between STA and each library. For SNMP, this test is required. For SCI, it is highly recommended.

To avoid dropped connections and lost library data, you should perform this procedure for each monitored library whenever you add or change connection settings for the library or the STA client.

1. Review When to Test the Library Connection. Because a connection test can cause a momentary loss of incoming library data, you should perform this procedure only when necessary.
2. In the STA GUI, expand the **Setup & Administration** tab, and then select **Library Connections**.
3. In the Monitored Libraries table, select a library, then click **Check / Test Connection** ✔.



4. The Connection Test Status message displays the results. Click **OK** to dismiss.

   For SNMP, the message indicates results for the following:

   - **MIB Walk Channel test**—Checks for library initialization, network connectivity, proper SNMP client settings, and correct library firmware.
   - **Trap Channel test**—Requests that the library send a test trap (13) to STA.
   - **Media Validation Support test**—Checks for the minimum library firmware and configuration required to support STA media validation.

   For SCI, the message indicates results for the following:

   - **STA-to-Library Communications**—Results of the SCI connectivity from STA to the SL4000 library.
   - **Library-to-STA Communications**—Results of the outbound SCI connectivity from the SL4000 to the STA server.
5. The Monitored Libraries table updates with the results of the test. See About the Monitored Libraries Table for a description of the fields.
6. If the test fails:
   - If the test fails because of a timeout, repeat this procedure during a period of lower library activity. Once the test completes, you can compare the timestamps to verify that the library is providing current information.

- If the OSCI test fails, see Enable and Test the SCI Destination on the SL4000.
- If the test fails for other reasons, see Troubleshoot the Library Connection.

7. After successfully testing the connection, proceed to Manually Collect Library Data.

When to Test the Library Connection

You should perform a connection test at specific times to ensure STA can receive library data.

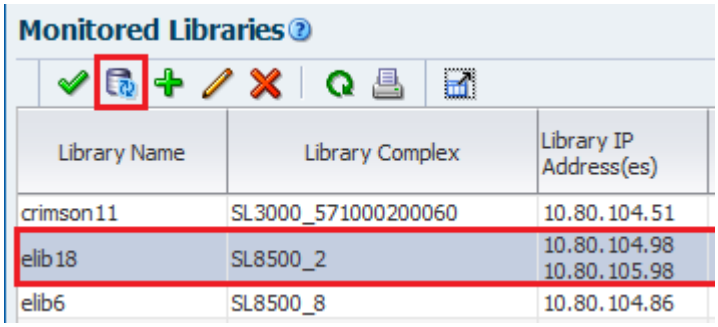
- After initial configuration of the connection between STA and a library. For SNMP, the test is required to populate the engine ID. For SCI, the test following initial configuration is highly recommended.
- After modifying any settings for the STA client or a monitored library.
- After rebooting a monitored library. Wait until the library is fully operational before initiating the connection test.
- After a redundant electronics switch has taken place on a SL3000 or SL8500 library. Wait until the switch has completed and the library is fully operational before initiating the connection test. See Update SNMP After a Redundant Electronics Switch (SL3000, SL8500).
- Anytime you suspect loss of data from one or more libraries.

Manually Collect Library Data

Initiate a manual data collection to begin monitoring the library with STA. You must also manually collect data for each monitored library whenever you add or change connection settings for the library or the STA client.

> **Note:**
>
> You can run up to five data collections simultaneously, but you must initiate them one at a time. Repeat this procedure as many times as necessary, selecting a different library each time

1. Review When to Manually Collect Data.
2. In the STA GUI, expand the **Setup & Administration** tab. Select **Library Connections**.
3. Select a library in the Monitored Libraries table, and then click **Get latest data** .



4. Click **OK** to dismiss the Information dialog.
5. Data collections may take several minutes to an hour depending on the library size. The status updates every four minutes, and the screen refreshes every eight minutes (the default interval). However, you can click **Refresh Table** at any time.
6. STA updates the Monitored Libraries table with the results. See About the Monitored Libraries Table.
7. Repeat this procedure as many times as necessary, selecting a different library each time.

When to Manually Collect Data

For STA to receive library data, and for STA to be notified of changes in the library environment manually collect data at these times.

Data collection is REQUIRED when:

- You configure a new library connection.
- You modify the connection settings in STA or on the library.
- A redundant electronics switch has occurred (for SL3000/SL8500 libraries).

Data collection is RECOMMENDED when:

- A large number of media are entered or ejected from a library, such as through an SL3000/SL4000 Access Module (AEM).
- A drive is added, removed, or swapped. For an added or swapped drive, wait 15 minutes after the drive has initialized. For a removed drive, wait about one minute after the removal.
- A robot is added, removed, or swapped.
- Library active storage regions or partitions are modified. Wait 15 minutes after the library controller database has been updated before manually collecting data.
- Anytime you suspect library configuration data is out of sync on STA.
- Anytime you suspect a data collection failed because of a reason external to STA.

About Library Data Collection

STA begins receiving library data as soon as you establish a connection to the library. However, the STA user interface does not display the data until STA builds the library configuration model.

To build the initial configuration model, you should initiate a manual data collection as soon as you establish the library connection. After the initial data collection, STA updates the library configuration model through scheduled and triggered data collections.

What is Collected During the Initial Data Collection

- Locations of activated storage cells
- Partition information

- Drive types, identifiers, and locations
- Media types, volume serial numbers (volsers), and locations

Depending on the size and activity level of the library, the initial data collection may take several minutes to over an hour. The STA user interface does not show a complete picture of the library environment and exchange activity until the data collection completes. During this time, you may see fluctuations in various analytic and summary data. This is normal.

How Data Collections Are Initiated

- *Scheduled*—A full collection of all library configuration data occurs automatically every 24 hours at a user-defined time. Schedule this during low levels of library activity.
- *Triggered*—STA automatically initiates data collections whenever it detects significant changes in the library state or configuration (for example, the addition of a drive or media, or a change in partition configuration). This is a partial data collection that updates only the library configuration affected by the change. For example, a data collection triggered by the addition of a new media, will only update the media configuration information. Triggered data collections take a short time.
- *Manual*—You can initiate a manual data collection at any time, as long as there is an active connection to the library. This is a full collection of all library configuration data. See Manually Collect Library Data.

Affect of Data Collections on Library Performance

The libraries process data collections at a lower priority than regular library operations, so data collections have little impact on library performance. However, performing a data collection during periods of heavy library activity can cause the data collection itself to take longer to complete. Oracle recommends that you perform scheduled and manual data collections during periods of lower library activity.

What Data is Collected from the Library

STA uses data received from the monitored libraries to created and maintain the STA data store. It includes the following information types.

- *Library configuration model* — A hierarchical view of the library and device configurations, properties, and statuses.
- *Exchange records* — Detailed information about all drive and media exchanges, including drive clean activities.
- *Errors and events* — Significant library errors and events.

About the Monitored Libraries Table

The Monitored Libraries table shows the current status of all libraries monitored by STA.

To access the table, expand **Setup & Administration** and then select **Library Connections**. The table has the following fields which are updated after a data collection or connection test.

Table Field	Description	Applies to:
Library Name	Name used to identify the library within STA.	SNMP, SCI
Library Complex	The identifier for the library complex. If this field is blank, it will be supplied after you perform a manual data collection.	SNMP, SCI

Table Field	Description	Applies to:
Library IP Address	The IP address of the monitored library.	SNMP, SCI
STA IP Address	IP address of the STA server.	SNMP, SCI
Library Engine ID	The unique SNMP engine ID for the library (see About the Library Engine ID).	SNMP only
Connection Type	Either SNMP or Library API (which is also known as SCI).	SNMP, SCI
Library API User ID	ID of the SL4000 user account to be used for SCI communication.	SCI only
Library API HTTP port	Port used for SCI HTTP communication. The default is 7102.	SCI only
Library API HTTPS port	Port used for SCI HTTPS communication. The default is 7103.	SCI only
Recent Communication Status	Indicates the latest status of information from the library over the outbound SCI channel or SNMP trap channel. This may intermittently indicate `MISSED HEARTBEAT`. This is normal.	SNMP, SCI
Library Time Zone	The time zone of the library.	SNMP, SCI
Last Successful Connection	Date and time when the test or data collection was completed, if successful.	SNMP, SCI
Last Connection Attempt	Date and time when the connection test or data collection was initiated.	SNMP, SCI
Last Connection Status	Results of the test or data collection. • IN PROGRESS – A data collection is underway. • SUCCESS – The connection test or data collection completed successfully. • FAILED – The connection test or data collection failed. Possible reasons are listed in the Last Connection Failure Detail field. • REJECTED – The data collection request was rejected, possibly because the library is busy or unavailable. • DUPLICATE – The data collection request was rejected because another one is already is progress.	SNMP, SCI
Last Connection Failure Details	If the test or collection fails, STA provides information on the cause of failure.	SNMP, SCI

About the Library Engine ID

Every SNMP v3 agent has a globally unique hexadecimal engine ID to identify the device. The Library Engine ID is a field updated and displayed in the Monitored Libraries table.

When you configure a new SNMP connection on STA, leave the library engine ID blank. Then when you test the SNMP connection to the library, STA automatically retrieves the library engine ID and displays it in the Monitored Libraries table.

The Library Engine ID field may be blank if:

- This is a new library connection, and you have not yet tested the connection.

- You have modified an existing library connection. In this case, STA automatically clears the Library Engine ID field to indicate that the connection has been dropped and you must perform a new connection test.
- The connection with the library has been dropped for any reason.

When to manually clear the Library Engine ID field:

Never modify the library engine ID value. However, you should manually clear the value at the following times.

- If a connection test fails—in particular, if the error message indicates a failed trap channel test—you should clear the library engine ID before retesting the connection.
- After a library firmware upgrade, you should clear the engine ID and perform a connection test.

Troubleshoot the Library Connection

Diagnose and resolve issues with the SNMP or SCI connection between STA and a monitored library.

General Troubleshooting

- Verify the Library is Operational

SCI Troubleshooting

- Verify the Firewall Settings
- Enable and Test the SCI Destination on the SL4000
- Manually Configure the SL4000 to Send Outbound SCI to STA

SNMP Troubleshooting

- Export SNMP Connection Settings to a Text File
- Display All SNMP Trap Recipients
- Troubleshoot a Failed MIB Walk Channel Test
- Troubleshoot a Failed Trap Channel Test
- Troubleshoot a Failed Media Validation Support Test
- Troubleshoot Unsuccessful Trap Processing
- Verify SNMP Communication with a Library (optional)

Verify the Library is Operational

Verify that the library is fully initialized and operational. You should verify the library state before doing a library connection test or data collection, as these processes will fail if the library is not fully initialized.

> **Note:**
>
> If you are configuring multiple library connections at one once, to minimize library disruption, complete this procedure for all libraries before testing the connections.

SL150 or SL4000

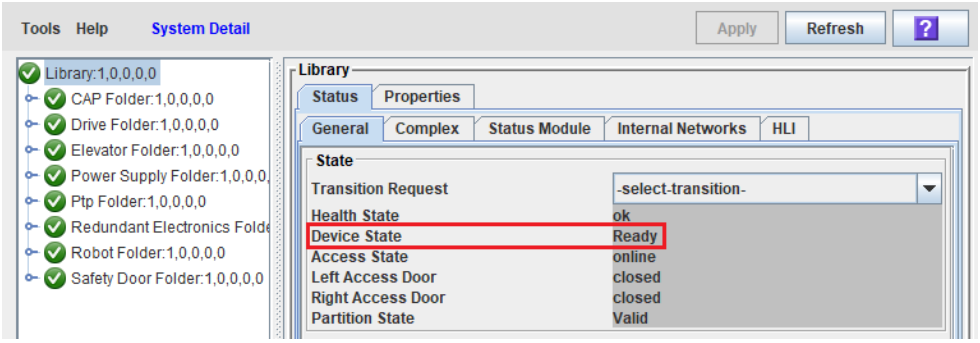
1. Log in to the browser-based user interface.
2. At the top of the screen, verify that the Health field indicates "`Operational`".

SL500

1. Log in to the library with SLC.
2. In the **Tools** menu, select **System Detail**.
3. In the navigation tree, select **Library**.
4. Select the **Status** tab.
5. Verify the library Operational State indicates "`Operational`".

SL3000 and SL8500

1. Log in to the library with SLC.
2. In **Tools** menu, select **System Detail**.
3. In the navigation tree, select **Library**.
4. Select the **Status** tab, then select the **General** tab.
5. Verify the Device State indicates "`Ready`".



Verify the Firewall Settings

For the SL4000 and STA to communicate using SCI, the firewall settings must be properly configured.

1. Verify the following firewall settings:
   - Firewall is running
   - Check hosts.allow and hosts.deny files if using those OS services
   - REJECT rules are not interfering with the inbound and outbound SCI ports (such as 7103, 7102, and 7026)
   - Port forwarding from 162 to 7029 (port 7029 may be different if you have customized it)
   - Network router configuration between the STA server and library

   To verify, open a terminal session and login as the root user. Issue the following:

   ```
   # systemctl status iptables
   # more /etc/hosts.allow
   # iptables -L
   ```

2. If needed, use the iptables command to remove or modify the firewall rules to allow SCI communication. For example:

   ```
   # iptables -D INPUT 5
   ```

   > **WARNING:**
   >
   > Removing or modifying firewall rules can create security risks and must be done by a qualified security administrator.

3. Verify the iptables settings:
   a. Verify iptables rules were been saved correctly using the service iptables save command.

      ```
      # service iptables save
      ```

   b. Verify the iptables server is enabled. For example:

      ```
      # systemctl status iptables
      # systemctl start iptables
      # systemctl enable iptables
      ```

Enable and Test the SCI Destination on the SL4000

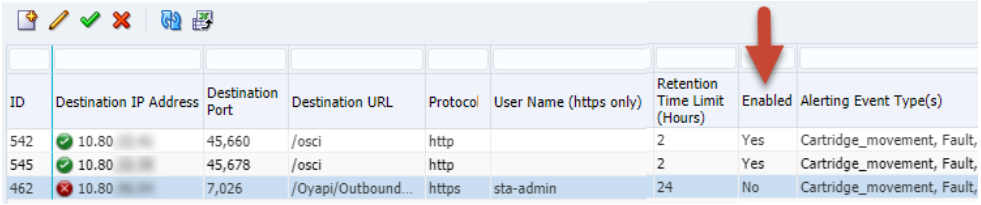
Verify the SCI destination is enabled and run a test to validate the configuration to the STA server is properly defined. The test sends a "test" event message to the destination.

Access the SL4000 GUI Notifications Page

1. Log into the SL4000 GUI.
2. Click **Notifications** in the left navigation area.
3. Click the **SCI** tab.

Verify the Destination is Enabled

1. Verify the **Enabled** column for the STA destination says **Yes**.



2. If not, select the STA destination in the table and then click **Edit** .
3. Check the **Enabled** box, and then click **Ok**.

Test the Destination

1. Select the STA destination in the table.
2. Click **Test** , and then confirm the test.
3. If the test fails, you may need to manually configure the destination. See Manually Configure the SL4000 to Send Outbound SCI to STA.

Manually Configure the SL4000 to Send Outbound SCI to STA

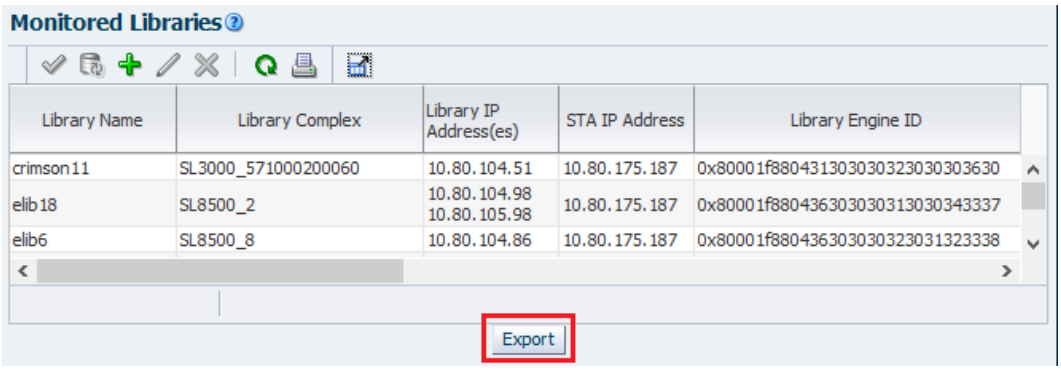
STA automatically configures the outbound SCI connection. However, if there are SCI connections issues you may need to manually configure the connection.

1. STA automatically configures OSCI when you add the SL4000 to the Monitored Libraries table within the STA interface. Only perform this procedure if you are troubleshooting a connection issue.
2. Sign in to the SL4000 GUI.
3. Click **Notifications** in the left navigation area.
4. Click the **SCI** tab.
5. Click **Add** .
   - **Protocol** - Select https.
   - **Username and password** - Credential information for an STA user account to be used by the SL4000 to communicate to STA using outbound SCI.
   - **IP address** - Enter the IP address for the STA server.
   - **Destination Port** - Set to 7026.
   - **Destination URL** - Set to /Oyapi/OutboundWebServicePort
   - **Retention Time Limit** - Set to 24 hours.
   - **Alerting Event Types** - Select "All"

Export SNMP Connection Settings to a Text File

Export SNMP connection information to a text file to help troubleshoot connection issues or re-enter connection information.

1. In the left navigation, expand **Setup & Administration**, then select **Library Connections**.
2. At the bottom of the screen, click **Export**.



The file is saved with the name `SnmpConfiguration.txt`. Passwords are not included in the file.

Example 6-1 Sample SNMP Configuration File

```
Define SNMP Client Settings
---------------------------

Client Attributes
-----------------

STA SNMP Connection Username (Auth) = abc1
Connection Password Encryption (Auth) = Not Specified
Connection Password Encryption (Auth) = SHA
Privacy Encryption Password (Privacy) = Not Specified
Connection Password Encryption (Auth) = DES
STA Engine ID = 0x8000002a050000014817ec1dc1
SNMP Trap Levels = 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
Trap Community = public
User Community = public
V2C Fallback = false

Monitored Libraries
-------------------

STA IP Address = 10.80.145.78
Library Name = SL3000A
Library Complex = SL3000_5720123200089
Library Primary IP Address = 10.80.104.51
Library Secondary IP Address = Not Specified
Library Engine ID = 0x80001f8804313030301231233030000
Requested MIB Walk Time = 00:00:00
Library Serial Number = 5720123200089
Library Time Zone = UTC
```

```
Recent SNMP Trap Communication Status = GOOD
Last Connection Status = SUCCESS
Last Connection Failure Detail = Not Specified
```

Display All SNMP Trap Recipients

Display all trap recipients defined on the library and verify the settings.

SL150

1. Log in to the browser-based user interface.
2. In the navigation tree, select **SNMP**, then select **SNMP Trap Recipients** to display a list of trap recipients.

SL500, SL3000, and SL8500

1. Log in to the library CLI.
2. Issue the following command:

   `snmp listTrapRecipients`

   For example:

   ```
   ADMIN> snmp listTrapRecipients
   requestId
   requestId 1
   ...
   Index 1
   ...
   Object Snmp snmp
   Done
   Failure Count 0
   Success Count 1
   COMPLETED
   ```

3. Note the index number of the STA trap recipient in the displayed output. In the example above, the index number is "1".

Troubleshoot a Failed MIB Walk Channel Test

The MIB Walk Channel test checks for library initialization, network connectivity, proper SNMP client settings, and correct library firmware.

If this test fails, one or more of the following issues could be the cause:

- STA is not configured.
- The library is not initialized.
- The library firmware does not meet the minimum for STA.
- There are network problems between the STA server and library.
- A static IP address is not assigned to the STA server or library.
- SNMP is not enabled on the library.
- SNMP client settings do not match between STA server and library.

Steps to Perform on the Library

1. Log in to the library CLI.
2. Verify that the library is fully initialized and not super busy. See Verify the Library is Operational.
3. Check communication from the library to the STA server. This command is not available on the SL150.
   - SL8500 and SL3000:

     ```
     traceRoute <IP address of STA server public port>
     ```

   - SL500:

     ```
     traceroute <IP address of STA server public port>
     ```

   The output shows the number of hops and the round-trip time to reach each one. The round-trip time (the last line in the command output) should be less than one second. If it is not, confirm the network's performance with your network administrator.
4. Verify that SNMP has been enabled on the public port. See Enable SNMP on the Library.
5. Verify that the SNMP v3 user was added correctly:
   - On SL500, SL3000, and SL8500 libraries, use the `snmp listUsers` command to view a list of SNMP users. On SL150 libraries, in the navigation tree, select **SNMP**, then select **SNMP Trap Recipients**.
   - To add an SNMP v3 user, see Create an SNMP v3 User.
6. Verify that a static IP address has been assigned to the library. See Retrieve the Library IP Address.
7. After performing all other steps on both the library and STA server, consider deleting and re-adding the SNMP v3 user.

Steps to Perform on the STA Server

1. Log in to the STA server.
2. Verify that the STA server is using a static IP address.
3. Check communication from the STA server to the library.

   ```
   # traceroute -I <IP address of library public port>
   ```

   The output shows the number of hops and the round-trip time to reach each one. The round-trip time (the last line in the command output) should be less than one second. If it is not, confirm the network's performance with your network administrator.
4. To verify that the STA server can reach the library public port, ping the primary library IP address and, if applicable, the secondary IP address.
5. Verify that UDP ports 161 and 162 are enabled on all network nodes between the STA server and the library. See Verify SNMP Communication with a Library (optional) for instructions.
6. Verify that the settings on the STA SNMP Client Attributes screen exactly match the corresponding settings for the SNMP v3 user and trap recipient on the library. See Configure SNMP Client Attributes for STA for instructions.
7. Verify that the settings on the STA Monitored Libraries screen are correct for the library. See Configure the SNMP Connection to a Library for instructions.

Troubleshoot a Failed Trap Channel Test

The Trap Channel test requests that the library send a test trap (13) to the STA server. If the test fails, STA indicates the date and time when the last trap or inform was received.

If the test fails or indicates `Unknown`, one or more of the following issues could be the cause:

- The library firmware does not support the test trap.
- STA is not properly configured as a trap recipient on the library.
- If you recently upgraded to STA 2.0.x or above, the STA server's IP address is not specified in the connection details for the library.

Use this procedure to diagnose and resolve the issues.

1. Verify that the library is running the recommended or higher firmware. Lower firmware versions may not support the test trap (13).
2. After upgrading to STA 2.0.x or above, verify that you have selected the STA server's IP address in the library's connection details. See Configure the SNMP Connection to a Library for instructions.
3. Use the `snmp engineId` (for SL500 libraries) or `snmp engineId print` (for SL3000 and SL8500 libraries) command to display the library engine ID. (Not applicable to SL150 libraries.)
4. Verify that STA is configured correctly as a trap recipient. See Display All SNMP Trap Recipients for instructions.
   - **Engine Id** - Must match the library engine ID displayed in the step above. The entry must not contain any upper-case characters. For the SL8500 and SL3000 libraries, the entry must include the 0x prefix (the SL500 may also show this prefix).
   - **Host** - IP address of the STA server.
   - **Version** - Must be `v3`.
   - **Auth** - Must be `SHA`.
   - **Priv** - Must be `DES`.
   - **Auth Pass** and **Priv Pass** - Must match the passwords on the STA SNMP Client Attributes screen, as well as the passwords specified when creating an SNMP user. For SL500 libraries, verify that the passwords do not contain single quotes as text.
   - **Trap Level** - Must include trap 13.
5. Verify that the library engine ID matches the value in the STA Monitored Libraries screen. See Configure the SNMP Connection to a Library for details.

   If it does not match, clear the `Library Engine ID` field on the screen, and then perform a library connection test. See Test the Library Connection for instructions.

Troubleshoot a Failed Media Validation Support Test

The Media Validation Support test checks for the minimum library firmware and configuration required to support STA media validation.

If the library configuration does not support media validation, the test reports `Not Applicable`. If the test is unsuccessful for a library that can support media validation, one or more of the following issues could be the cause:

- The library firmware does not support media validation.
- SNMP v3 is not configured.
- There are no drives in the media validation pool.
- There are no empty or reservable drives in the media validation pool.

Use the following procedure to diagnose and resolve the issues.

1. Verify that the library and drives meet the minimum firmware levels required for media validation.
2. Verify that you have an SNMP v3 user configured on both the library and STA server, and have configured the STA server to be a trap recipient on the library. Review the library SNMP configuration steps in the Configure SNMP on the Libraries and Configure SNMP on the STA Server.

Troubleshoot Unsuccessful Trap Processing

Troubleshoot an issue if traps are not being received by the STA server, or traps are not being processed by STA.

1. Log in to the STA server as the system root user.
2. Verify that the STA server is using a static IP address.
3. Monitor TCP/IP packets sent between the STA server and the library.

   ```
   # tcpdump -v host <IP address of library public port> > /var/tmp/<output file name> &
   ```

4. In the output, look for `.snmptrap` and `SNMPv3`. Network traffic for data collection requests contain `.snmp`.

   If there is activity on the library, but no traps are being received, check the library trap recipient entry for accuracy. See Troubleshoot a Failed Trap Channel Test.

5. Verify that SNMP port 162 is available for STA. The STA trap listener processes traps through this port.

   If necessary, troubleshoot communications over this port:

   a. Check the `/Oracle_storage_home/Middleware/user_projects/domains/tbi/servers/staAdapter/logs/staAdapter.log` file for a "SEVERE" error, such as:

      ```
      "SEVERE: SNMP Trap/Inform Listener Port 162 is NOT bindable. Stop the application currently bound to that port."
      ```

   b. If port 162 is already in use, determine what process is using it.

      ```
      # netstat -ap |grep -I snmp
      # netstat -anp |grep ":162"
      ```

c. Follow the process associated with the port, or check what services may have started during system boot.

```
# chkconfig --list
```

6. If the `snmpd` or `snmtrapd` services are running, ensure they are disabled:

a. Deconfigure SNMP services.

```
# systemctl stop snmpd
# systemctl stop snmptrapd
```

b. Stop SNMP services.

```
# systemctl disable snmpd
# systemctl disable snmptrapd
```

c. Stop and restart STA services.

```
# STA stop all
# STA start all
```

7. If some traps are being reported in the STA Notifications screen, verify that all trap levels were specified when creating a trap recipient on the library. See the SNMP v3 trap recipient creation procedure in the Create the STA SNMP v3 Trap Recipient for the list of supported trap levels.

8. For the SL500, verify that you configured the library with a supported version of SL Console. Earlier versions of SL Console restrict the number of trap level characters that can be entered.

9. For SL500 and SL150 libraries, verify that the Volume Label Format is set properly.

7

Upgrade to STA 2.4.0

Upgrade from any previously released version of STA to version 2.4.0. To upgrade, you must deinstall the current STA version, install the new version, and then convert the existing database to the new schema.

- Prepare STA for the Upgrade
- Upgrade STA
- Configure STA After the Upgrade

Prepare STA for the Upgrade

Make sure STA is ready for the upgrade. Record all important information needed to configure the new version of STA.

- Understand What Occurs During the Upgrade
- Determine the Current Version of STA
- Verify the Environment Meets Requirements
- Review Environmental Changes for Upgrades from STA 2.0.x and Earlier
- Verify STA is Functioning Normally
- Save Existing Logs (optional)
- Record Current STA Users (optional)
- Rename Custom Templates that Use the STA– Prefix (optional)
- Record Current Custom Template Settings (optional)
- Record Executive Report Policy Settings (optional)
- Record Logical Group Ownership Settings (optional)

Understand What Occurs During the Upgrade

Before beginning an upgrade, familiarize yourself with all upgrade information and identify the instructions that apply to your site.

The upgrade transforms the existing STA data to be compatible with the new version of STA. After the upgrade, the STA processes new data according to the new schema and analytics rules. Historical data is not reprocessed.

Be sure to allocate sufficient time for the entire process. While you are performing the upgrade, STA does not receive exchange information from the monitored libraries. The new version of STA does not begin receiving information from the libraries until after you have completed all upgrade and post-upgrade configuration steps, including testing the SNMP connection to each monitored library.

Some upgrade preparation tasks may require you to coordinate with other groups at your site, such as network administration. You should have all preparation tasks done in advance so you can complete the upgrade in as little time as possible.

Use the Record Installation and Upgrade Information to organize your upgrade activities and record your settings.

Determine the Current Version of STA

Use the GUI to determine the version of STA currently running on the server. If running 2.0.x or below, there are special considerations for the upgrade.

1. Log in to STA using an STA administrator username.
2. Click **About** in the Status Bar. Note the STA version.

Verify the Environment Meets Requirements

Ensure that your environment meets all STA prerequisites.

1. Verify that your site and the target server meet the Requirements for STA . Be sure to allocate sufficient time for the entire process.
2. Ensure the `/tmp` file system on the target STA server has sufficient space for the upgrade. The size of `/tmp` should be at least as large as the size of your existing uncompressed STA database; a minimum of 4 GB is required, and for large databases, Oracle recommends you increase the size of `/tmp` to 32 GB, at minimum.
3. Ensure that all required RPM packages are installed on the STA server. See Install Required Linux Packages for instructions. As a final check, the STA installer will also notify you if any packages are missing.
4. Review the file system structure on the STA server and verify that the required users and groups have proper access to the locations used by the STA installer. See Table 3-1 and Users, Groups, and Locations Used by the STA Installer.

Review Environmental Changes for Upgrades from STA 2.0.x and Earlier

Review the environmental changes that apply to your site and impact the upgrade. These changes apply only to upgrades from 2.0.x or earlier.

Verify you have the correct Linux version

You will need to install a new version of Linux as part of the STA upgrade process:

STA 2.4.0 is supported on Oracle Linux 7.8 and 7.9.You will have to install this version of Linux before upgrading STA. You may also need to install or update the required Linux RPM packages—as part of the upgrade preparation, you will ensure that all required RPM package levels are installed, and as a final check, the STA installer will also notify you if any packages are missing.

Check the default WebLogic port numbers

Changes to the default WebLogic Administration console port numbers were introduced in STA 2.1.0. If you are currently using the old default port numbers, you

may want to change to the new default values. The new and old default port numbers are as follows:

- New defaults for STA 2.1.0 and later—7019 (HTTP) and 7020 (HTTPS)
- Old defaults (STA 1.0.x and STA 2.0.x)—7001 (HTTP) and 7002 (HTTPS)

> **Note:**
>
> The WebLogic Administration console ports are external. Your network administrator may need to configure firewalls and routers to open communication between the STA server and the clients accessing the WebLogic Administration interface.

Note the change in username and password requirements

Following are the username and password requirements for STA and MySQL. You may need to coordinate these requirements with any internal requirements at your site.

Username requirements are as follows:

- Must be 1–16 characters in length
- All usernames must be unique

Password requirements are as follows:

- Must be 8–32 characters in length
- Must include at least one uppercase letter and one number
- Must not include spaces or tabs
- Must not include any of the following special characters:

```
% & ' ( ) < > ? { } * \ ' " ; , + = # !
```

Verify the required ports for STA managed servers

The default STA managed server port numbers STA 2.0.x and later are as follows:

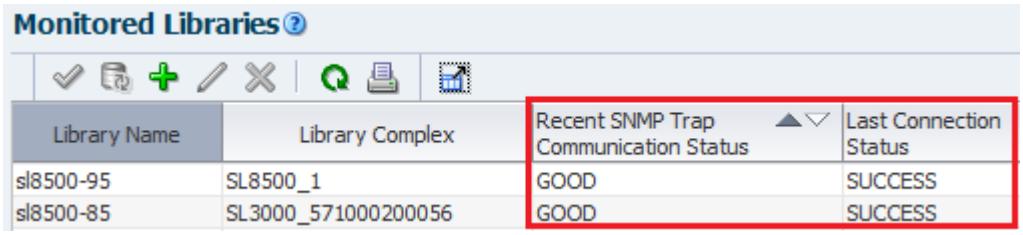
- StaUi—7021 (HTTP) and 7022 (HTTPS)
- StaEngine—7023 (HTTP) and 7024 (HTTPS)
- StaAdapter—7025 (HTTP) and 7026 (HTTPS)

> **Note:**
>
> The StaUi ports are external. Your network administrator may need to configure firewalls and routers to open communication between the STA server and the clients accessing the STA user interface.

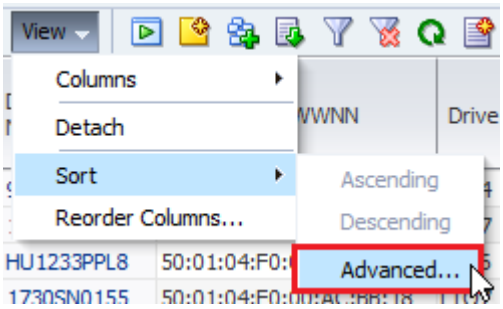
Verify STA is Functioning Normally

Verify that your current STA environment is functioning normally before upgrading.

1. Verify STA has had recent, successful communication with each monitored library.
   a. Log in to STA as an administrator user.
   b. Expand the **Setup & Administration** tab, select **SNMP Connections**.
   c. Verify the following values in the Monitored Libraries table:
      - Recent SNMP Trap Communication Status—GOOD
      - Last Connection Status—SUCCESS



2. Verify that STA is processing exchanges across all libraries.
   a. Expand the **Tape System Activity** tab, select **Exchanges – Overview**.
   b. Click **Filter** . Add **Exchange End (No. Days) | Less than # days ago | 1**.
   c. Click **Apply**.
   d. From the table's **View** drop-down menu, select **Sort** and then **Advanced...**



   e. Sort by Drive Library Name, Drive Serial Number.
   f. Verify that all libraries have exchange activity.

Save Existing Logs (optional)

Save any logs you want to keep since existing application and service log bundles are not retained after the upgrade.

1. Locate any installation and database logs you want to retain, and move them to a safe place. Logs that may be of interest are located in the STA logs location you have defined for your installation. See Review the STA File System Layout for details.
2. Create an RDA log bundle on the current STA installation.
   a. Log in to STA as an administrator user.
   b. Expand the **Setup & Administration** tab, select **Logs**.

c. Click **Create New Log Bundle**  .

d. Assign a bundle name and click **Save**. It may take several minutes for the process to complete.

3. Download the RDA log bundle you just created, as well as any others you want to retain. You must download the bundles one at a time.

   a. In the Service Logs table, select the bundle you want to download.

   b. Click **Download Selected Log Bundle**  .

   c. Save the log bundle to an accessible location.

Record Current STA Users (optional)

Display and record the current user configuration to reuse them in the upgraded version of STA.

- Record MySQL Usernames
- Record STA SNMP Client Settings
- Record WebLogic Usernames—Upgrades from STA 1.0.x Only
- Record STA Usernames—Upgrades From STA 2.0.x or Later
- Record STA Email Server Settings

Record MySQL Usernames

Record existing MySQL usernames used to access the STA database. You cannot retrieve the passwords.

1. On the STA server, open a terminal session. Log in as the Oracle user.
2. Display all STA database usernames. For example:

```
$ mysql -uroot -p -e "select distinct(user) from user order by user ;" mysql
```

3. Record the usernames.

Record STA SNMP Client Settings

Record SNMP client settings for STA. You will reenter these values after the upgrade. In the new version of STA, the SNMP values must match what is specified on the monitored libraries.

1. Log in to STA as an administrator user.
2. Expand the **Setup & Administration** tab, select **SNMP Connections**.
3. In the Client Attributes table, record the values from the following columns:
   - SNMP Username
   - User Community
   - Trap Community

Record WebLogic Usernames—Upgrades from STA 1.0.x Only

For upgrades from STA 1.0.x, record existing WebLogic usernames used to log in to STA. You cannot retrieve the passwords.

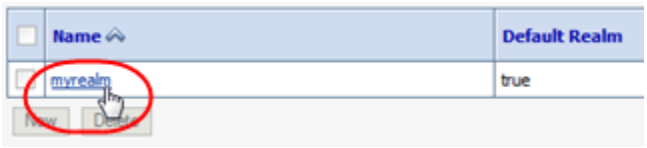
1. In a browser, go to the WebLogic administration console:

   http(s)://<*STA host_name*>**:**<*WebLogic port_number*>**/console/**

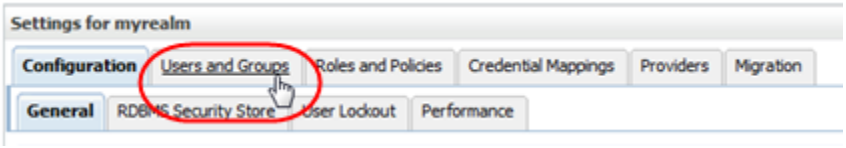
   For example: `https://staserver.example.com:7002/console/`

2. Log in using the WebLogic administration console username and password.
3. In the Domain Structure navigation tree, click **Security Realms**.

4. In the Name column, select the **myrealm** active link (do not select the check box).



5. Select the **Users and Groups** tab.



6. Within the Users table, record the usernames you want to retain.

Record STA Usernames—Upgrades From STA 2.0.x or Later

For upgrades from STA 2.0.x or later, record usernames used to log in to STA. You cannot retrieve the passwords.

1. Log in to STA as an administrator user.
2. Expand the **Setup & Administration** tab, select **Users**.
3. Record the usernames and roles you want to retain.

Record STA Email Server Settings

Record the STA email protocol and account username. You cannot display the password.

1. Log in to STA as an administrator user.
2. Expand the **Setup & Administration** tab, select **Email**.
3. In the SMTP Server Settings table, select the StorageTek Tape Analytics Alerts record. Click **Edit Selected SMTP Server** .

4. In the Define SMTP Server Details dialog, record the following values:
   - Use Secure Connection Protocol
   - Username

Rename Custom Templates that Use the STA– Prefix (optional)

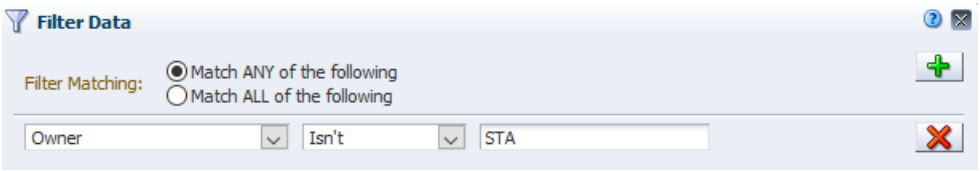
Rename any custom templates that have the prefix "STA-" to preserve them during the update. During the upgrade of STA, all templates with the "STA–" prefix are deleted and replaced by new STA predefined templates.

1. Log in to STA as an administrator user.
2. Expand the **Setup & Administration** tab, select **Templates Management**.
3. Sort the table by date Created/Updated, to focus on templates that have been modified since the STA installation date.
4. Select the text link of a custom template with name prefixed "STA-".
5. Click **Save Template** in the Templates Toolbar.
6. In the **Template Name** field assign a new name. Your entry must be unique.
7. Click **Save**.

Record Current Custom Template Settings (optional)

After the upgrade, all custom templates are preserved, but they are owned by the STA application ("STA") with public visibility. Record the current ownership and visibility settings so you can restore them after the upgrade, if necessary.

1. Log in to STA as an administrator user.
2. Expand the **Setup & Administration** tab, select **Templates Management**.
3. Filter to only display custom templates. Click **Filter** .
4. Select **Match ANY**, and add **Owner | Isn't | STA**.



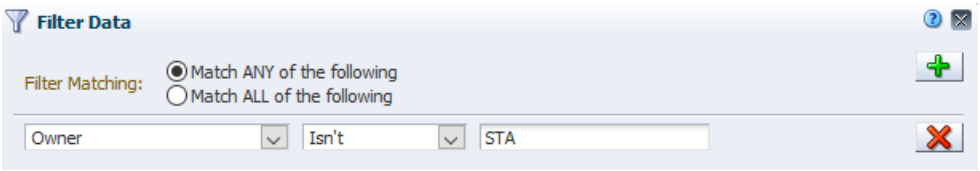
5. Click **Apply**.
6. Record the current Owner and Public Visibility settings for each custom template. If you have many templates, you may want to take a screen shot.

Record Executive Report Policy Settings (optional)

You only need to record executive report policy settings if STA has privately owned Executive Report policies. After the upgrade, all Executive Report policies are preserved, but they are assigned public ownership.

Use this procedure to record the current ownership settings for all private policies so you can restore them after the upgrade, if necessary. You can skip this procedure if Executive Report policy ownership is not critical to your implementation.

1. Log in to STA using an STA administrator username.
2. From the **Setup & Administration** tab, select **Executive Reports Policies**.
3. Filter to display privately owned policies. Click **Filter** .
4. Select **Match ANY**, and add **Owner | Isn't | STA**.



5. Click **Apply**.
6. Record the current Report Owner for each policy. If you have many policies, you may want to take a screen shot.

Record Logical Group Ownership Settings (optional)

After the upgrade, all existing logical groups are preserved, but they are owned by the STA application ("STA"). If you want to restore the ownership assignments after the upgrade, record the current ownership of the logical groups.

Logical group ownership is not critical to STA functioning, and any STA user with Operator or Administrator privileges can modify logical groups. Therefore, restoring the ownership assignments after the upgrade is not essential.

1. Log in to STA using an STA administrator username.
2. From the **Setup & Administration** tab, select **Logical Groups**.
3. Record the current Logical Group Owner for each group. If you have many policies, you may want to take a screen shot.

Upgrade STA

To upgrade STA, you must deinstall the current STA version, install the new version, and then convert the existing data and database to the new schema.

You can perform the upgrade by using a single-server or two-server method. The method chosen affects the order of the steps in the upgrade.

Before proceeding, review all tasks in Prepare STA for the Upgrade.

> **Caution:**
>
> Only a Linux administrator and STA administrator should perform the upgrade. All tasks are required and must be performed precisely as written in the order specified, or data loss could result.

- Decide on a Single-Server or Two-Server Upgrade
- Dump the Old STA Database (Task 1)
- Transfer the Old Database Dump (Task 2)
- Deinstall the Old STA Version (Task 3)
- Install the New Linux Version (Task 4)
- Install the New STA Version (Task 5)
- Dump the New STA Database (Task 6) - Optional
- Transfer the Old STA Database to the STA Server (Task 7)
- Process and Load the Old STA Database (Task 8)
- Upgrade the Old Database (Task 9)
- Recover a Failed Database Upgrade

Decide on a Single-Server or Two-Server Upgrade

Choose to use either one or two servers for the upgrade. The upgrade tasks are largely the same, but you will perform the tasks in a different order.

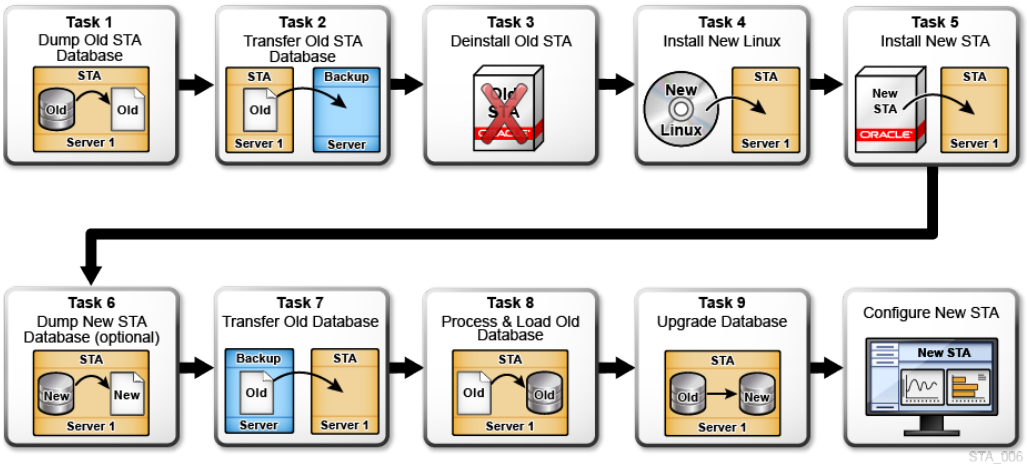
Considerations to help you decide on a method:

- **Single-server** — Does not require an additional dedicated server for the upgrade. If you do not need to install a new version of Linux, this method may be sufficient. However, STA is not monitoring libraries while you deinstall STA, upgrade STA, and then convert the database. Downtime is longer than with the two-server method.
- **Two-server** — Requires a second dedicated STA server. This method reduces application downtime since STA can continue to monitor libraries on the old server while you install Linux and STA on the new server. Even with this method, however, STA is not monitoring libraries while you convert the database. The length of downtime depends on the size of your current database.

Single-server Upgrade Process

For the single server method you perform Task 1 through Task 9 in sequential order.

Figure 7-1 Single-server Post-installation Upgrade Task Overview



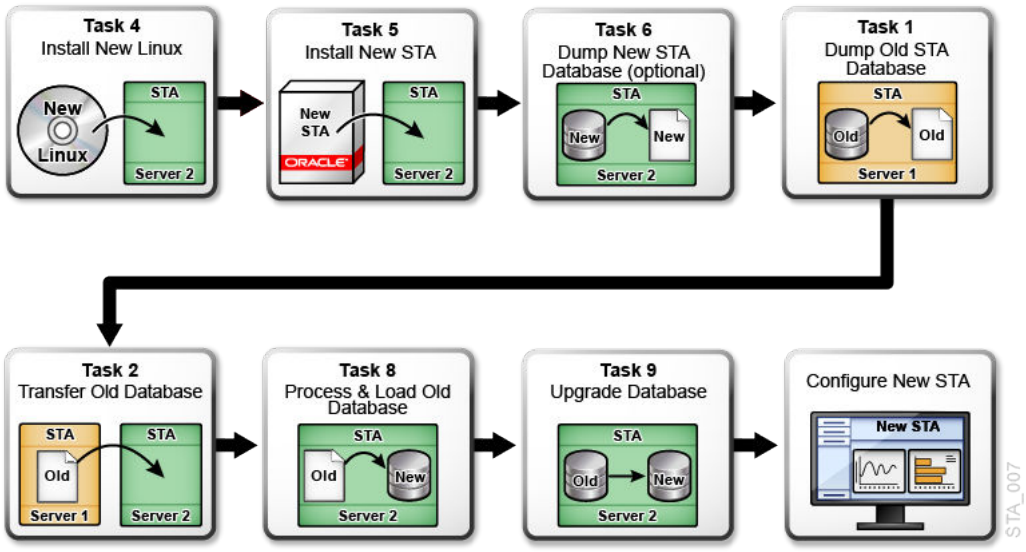
The single-server upgrade process is:

1. Dump the Old STA Database (Task 1)
2. Transfer the Old Database Dump (Task 2)
3. Deinstall the Old STA Version (Task 3)
4. Install the New Linux Version (Task 4)
5. Install the New STA Version (Task 5)
6. Dump the New STA Database (Task 6) - Optional
7. Transfer the Old STA Database to the STA Server (Task 7)
8. Process and Load the Old STA Database (Task 8)
9. Upgrade the Old Database (Task 9)
10. Reestablish connections to the monitored libraries, and perform necessary manual configuration tasks. Because the old version of STA must be deinstalled before you install STA 2.3.1, you must reenter some user configuration data manually.

Two-server Upgrade Process

In the two server upgrade, the order of the tasks is rearranged and Task 3 and Task 7 are omitted.

Figure 7-2 Two-server Upgrade Task Overview



The two-server upgrade process is:

1. Install the New Linux Version (Task 4)
2. Install the New STA Version (Task 5)
3. Dump the New STA Database (Task 6) - Optional
4. Dump the Old STA Database (Task 1)
5. Transfer the Old Database Dump (Task 2)
6. Process and Load the Old STA Database (Task 8)
7. Upgrade the Old Database (Task 9)
8. Reestablish connections to the monitored libraries, and perform necessary manual configuration tasks.

Dump the Old STA Database (Task 1)

Perform a full dump of the STA database before upgrading.

1. **IMPORTANT:** This is not the first task if using the two-server method. See Two-server Upgrade Process for the order of procedures.
2. Display the size of your current STA database.
   a. Log in to STA as an administrator.
   b. Click **About** in the Status Bar.
   c. Record the Database Current Size.
3. Verify that the location where you want to dump the database has sufficient space.
   a. On the STA server, open a terminal session. Log in as the Oracle user.
   b. Display the space available in the database dump destination, and verify it is sufficient for the dump file. For example:

```
$ df -h /dbdumpfiles
Filesystem                      Size  Used Avail Use% Mounted on
/dev/mapper/sta_server-STA_DbVol 200G   53G   243G  27% /dbdumpfiles
```

4. Stop all STA services: **$ STA stop all**
5. Start the MySQL service: **$ STA start mysql**
6. Dump the STA database into a single file (do not use the -v (verbose) option). Enter the database root user password when prompted.

   ```
   $ mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert
   --dump-date --events --flush-logs --routines --single-transaction --triggers
   --databases stadb > /dumpfile_path/dumpfile_name.sql
   Enter password: mysql_root_password
   ```

   In the following example, the STA 2.1.x database is dumped into the `/home/oracle` folder on the STA server with filename `Jan26_dump.sql`.

   ```
   $ mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert
   --dump-date --events --flush-logs --routines --single-transaction --triggers
   --databases stadb > /home/oracle/Jan26_dump.sql
   ```

7. To reduce the dump file size by approximately 50 percent, zip the file. For example:

   ```
   $ cd /home/oracle
   $ zip Jan26_dump.sql
   ```

Transfer the Old Database Dump (Task 2)

Transfer the compressed dump of the old STA database to either an off-platform backup server (single-server method) or the new STA server (two-server method). This is the second task in a single server upgrade, but a later task in the two-server method.

1. **IMPORTANT:** If you are upgrading from STA 2.3.0 or below with the single-server method, you must back up the STA database to another server. Do not backup the database to a file system on the current STA server, as the Linux installation in will destroy all data on the server.
2. If you have not done so already, stop all STA services: **$ STA stop all**
3. Record the checksum of the dump file. For example:

   ```
   $ cksum /home/oracle/Jan26_dump.sql.gz
   2169286306 37 /home/oracle/Jan26_dump.sql.gz
   ```

4. Transfer the file to the target server using a transfer utility such as SCP. The `-p` option preserves timestamp values.

   ```
   $ scp -p dump_file target_host:/path/
   ```

   In the following *single-server* example, SCP is used to transfer the compressed database dump file `Jan26_dump.sql.gz` to the `/dbdumpfiles` folder on backup host `backup1`. The `/dbdumpfiles` folder already exists on the backup host.

   ```
   $ cd /home/oracle
   $ scp -p Jan26_dump.sql.gz backup1:/dbdumpfiles
   ```

In the following *two-server* example, SCP is used to transfer the compressed database dump file `Jan26_dump.sql.gz` to the `/dbdumpfiles` folder on STA 2.3.1 host `sta_new`.

```
$ cd /home/oracle
$ scp -p Jan26_dump.sql.gz sta_new:/dbdumpfiles
```

5. On the target server, perform a checksum of the transferred file. Verify that the checksum values match. For example:

```
$ cd /dbdumpfiles
$ cksum Jan26_dump.sql.gz
2169286306 37 Jan26_dump.sql.gz
```

Deinstall the Old STA Version (Task 3)

You must deinstall the current version of STA.

> **Caution:**
>
> Uninstalling STA removes all STA data on the server. Make sure you have backed up the database if using the single-server method.

1. **IMPORTANT:** For the single-server upgrade method, make sure you have completed Dump the Old STA Database (Task 1) and Transfer the Old Database Dump (Task 2).
2. On the STA server, open a terminal session. Log in as the Oracle user that is a member of the Oracle group. You cannot deinstall STA as the Linux `root` user nor any other user with superuser privileges.
3. Change to the installer binary directory with the STA home directory. For example:

```
$ cd /Oracle/StorageTek_Tape_Analytics/oui/bin
```

4. Select either the wizard or silent mode to deinstall STA. Use the following commands to launch the deinstallation.
   - **Wizard:**

     ```
     $ ./deinstall.sh
     ```

     After launching the wizard, see Deinstall Using the Wizard. This mode requires an X11 display. See Installation Wizard Display Requirements for instructions.
   - **Silent-mode:**

     Before running silent mode, you must create a response file. See Create a Response File.

     ```
     $ ./deinstall.sh -silent -responseFile <absolute path to responsefile>
     ```
5. After completing the wizard or silent-mode deinstaller, verify the deinstallation was successful by listing the contents of the Oracle storage home directory. It should be empty.

   For example:

```
$ ls -la /Oracle
total 8
drwxr-xr-x   2 oracle oinstall 4096 Sep 23 14:55 .
```

```
dr-xr-xr-x. 31 root   root     4096 Sep 23 16:41 ..
$
```

Install the New Linux Version (Task 4)

STA 2.4.0 is supported on Oracle Linux 7.8 and 7.9. If the server is not running this version, you must upgrade it. If the server is already running a supported Linux version, skip this procedure.

> **Caution:**
>
> Installing a new operating system destroys all data on the server. Make sure you have backed up the database if using the single-server method.

1. For a two-server upgrade, this is the first task performed. For the single-server upgrade method, make sure you have completed Dump the Old STA Database (Task 1) and Transfer the Old Database Dump (Task 2).
2. Install a supported version of Linux.

   See Install and Configure Linux on the STA Server for instructions.

Install the New STA Version (Task 5)

Install the new version of STA on the server.

1. See Install STA for instructions.
2. Once installed, log into STA to verify it is working properly. Because the upgrade process is not yet complete, the Dashboard panes display the message "No data to display". This is normal. The library data will display after you upgrade the database and configure the new STA version.
3. Log out of STA.
4. On the STA server, open a terminal session. Log in as the Oracle user.
5. Stop all STA services:

   ```
   $ STA stop all
   ```

Dump the New STA Database (Task 6) - Optional

Dumping the new database is optional but recommended. If the database upgrade fails, you can restore the empty database to recover STA as if it were newly installed with no data.

1. On the STA server, open a terminal session. Log in as the Oracle user.
2. If you have not done so already, stop all STA services:

   ```
   $ STA stop all
   ```

3. Start the MySQL service:

   ```
   $ STA start mysql
   ```

4. Create the database backup file (do not use the -v (verbose) option). Enter the database root user password when prompted.

```
$ mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert --
dump-date --events --flush-logs --routines --single-transaction --triggers --
databases stadb > /dumpfile_path/dumpfile_name.sql
```

In following example, the STA database is dumped to the `/home/oracle` folder on the STA server with filename `STA_FRESH_INSTALL_BACKUP.sql`.

```
$ mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert --
dump-date --events --flush-logs --routines --single-transaction --triggers --
databases stadb >  /home/oracle/STA_FRESH_INSTALL_BACKUP.sql
```

If you see, "Can't connect to local MySQL server," the MySQL server is not running. Make sure you have started MySQL.

Transfer the Old STA Database to the STA Server (Task 7)

In the single-server upgrade method, transfer the backup of the old database to the STA server.

1. Only perform this procedure if using the single-server method. Skip if using the two-server method.
2. Stop all STA services on the STA server:

```
$ STA stop all
```

3. Transfer the database. The `-p` option on for SCP preserves timestamp values.

```
$ scp -p backup_host:/path_to_dump_file/dump_file_name.sql.gz /local_path
```

In the following example, SCP is used to transfer the compressed database dump file `Jan26_dump.sql.gz` from `/dbdumpfiles` on host `backup1` to the `/home/oracle` folder on the STA server.

```
$ scp -p backup1:/dbdumpfiles/Jan26_dump.sql.gz /home/oracle
```

4. Perform a checksum of the transferred file. Verify the checksum value matches the one you received when creating the database dump. For example:

```
$ cd /home/oracle/
$ cksum Jan26_dump.sql.gz
2169286306 37 /Jan26_dump.sql.gz
```

Process and Load the Old STA Database (Task 8)

Decompress the old database and reinstate it on the STA server. The decompressed database may require 10 to 15 times as much space as the compressed database.

1. Stop all STA services on the STA server:

```
$ STA stop all
```

2. Decompress the backup file. For example:

```
$ cd /home/oracle
$ unzip Jan26_dump.sql.gz
```

3. Purge the STA database of obsolete data, such as processed SNMP records and empty analytics records.

> **Note:**
>
> A permanent record of `purgerecs` command activity is saved in the STA database. Starting with STA 2.0, database purging also occurs automatically at runtime. Periodically, the MySQL Event Scheduler purges records from various tables to attenuate database growth.

a. Change to the STA database updates directory.

```
$ cd /<Oracle_storage_home>/StorageTek_Tape_Analytics/db/updates
```

b. Initiate the purge (for help with `purgerecs`, use **`$ ./purgerecs -h`**).

```
$ ./purgerecs /path_to_dump_file/dump_file_name.sql /path_to_dump_file/
dump_file_name_PURGED.sql
```

In following example, `purgerecs` processes the MySQL dump file `Jan26_dump.sql` in `/home/oracle`. The output is directed to a new file named `Jan26_dump_PURGED.sql` in `/home/oracle`.

```
$ cd /Oracle/StorageTek_Tape_Analytics/db/updates
$ ./purgerecs /home/oracle/Jan26_dump.sql /home/oracle/
Jan26_dump_PURGED.sql
```

4. This step is optional. Determine the database file size and estimate the load process time.

```
$ ls -s -h dump_file_name_PURGED.sql
```

5. Start the MySQL server:

```
$ STA start mysql
```

6. Load the old STA database (do not use the -v (verbose) option). Enter the database root user password when prompted. There is no command output as the process runs.

```
$ mysql -uroot -p -e "SET SESSION SQL_LOG_BIN=0; SOURCE /path_to_dump_file/
dump_file_name_PURGED.sql;"
Password: mysql_root_password
```

Where:

- `-p`—Prompts for the database root password established during STA installation.
- `-e`—Execute the following quote-enclosed statements:
  - `SET SESSION SQL_LOG_BIN=0;`—Turns off unnecessary binary logging, speeding up the load.
  - `SOURCE /path_to_dump_file/dump_file_name_PURGED.sql`—Loads the dump file into the DB.

If the command is successful, you are returned to the command prompt once the process completes.

Upgrade the Old Database (Task 9)

Upgrade the old STA database schema to the latest one for STA.

If upgrading from several levels down, the upgrade script will automatically perform multiple transformations until the database is up to the latest schema.

1. Stop all STA services:

   ```
   $ STA stop all
   ```

2. If you determined in Verify the Environment Meets Requirements that the size of `/tmp` is not sufficient for the upgrade, increase the size of `/tmp` as necessary.

   If this is not possible, set an environment variable for MySQL to use an alternate temp location:

   a. Create an alternate temp location and assign open permissions to it. For example:

      ```
      $ mkdir /dbbackup/tmp
      $ chmod 777 /dbbackup/tmp
      ```

   b. Stop MySQL: **$ STA stop mysql**

   c. Edit the MySQL configuration file. For example:

      ```
      $  vi /etc/my.cnf
      ```

   d. In the `mysqld` section of the file, add a line defining the alternate temp location, which is identified by the `tmpdir` variable. Following is an example of the file after this line has been added.

      ```
      [mysqld]
      #----- mysqld MySQL Server Options -------------------------

      tmpdir                          = /dbbackup/tmp
      server-id                       = 1
      ...
      ```

   e. Restart MySQL: **$ STA start mysql**

3. Change to the database updates directory.

   ```
   $ cd /<Oracle_storage_home>/StorageTek_Tape_Analytics/db/updates
   ```

4. Start the upgrade script.

   For example:

   ```
   $ ./upgradedb.sh
   ```

5. Wait until you see the finish banner before proceeding.

   ```
   +-------------------------------------------------------------+
   | Started.................2021-04-09 08:15:31                |
   | Finished................2021-04-09 08:17:51                |
   | Elapsed Time............01:52:26                            |
   | Starting Version........65.00r0                            |
   | Final Schema Version....74.00r0                            |
   | Schema Release Date.....2021-04-07 17:06:02                |
   | Records (approximate)...4,819,802                          |
   +-------------------------------------------------------------+
   ```

   The log files in **/var/log/tbi/install** also contain a record of the upgrade progress. If you previously upgraded the database with sudo or root access, the log files were created

with root ownership. Now, if you upgrade using the oracle user, you may see the following message (where the ## can vary):

```
/usr/bin/mysql: Can't create/write to file '/var/log/tbi/install/
apply_updates##.log' (Errcode: 13 - Permission denied)
```

This error results from the oracle user trying to update the log file which has root ownership. The error causes no problem for the actual database upgrade and the success of the upgrade can be verified in the finish banner.

6. If you increased the size of `/tmp` or created an alternate temp location, restore it to its normal size and location.
7. Start all STA services:

   ```
   $ STA start all
   ```

8. This step is optional. Delete the `STA_FRESH_INSTALL_BACKUP.sql` file to free up disk space on the STA database backup volume.
9. To check the level of the database, log into the STA GUI and click **About...** in the bottom right of the screen. Verify the Current Database Schema Version: 74.00.

Recover a Failed Database Upgrade

If the database upgrade does not complete successfully and repeated attempts to upgrade have also failed, you can attempt to recover.

1. **IMPORTANT:** Only perform this procedure under the direction of your Oracle support representative.
2. Repeat the last step of Process and Load the Old STA Database (Task 8) through Upgrade the Old Database (Task 9).

   If the upgrade fails again, the database is in an unknown, possibly damaged state and you should restore the database to its original, freshly installed state. Proceed to the next step.
3. Delete the damaged upgraded database.

   ```
   $ mysql -u root -p -e 'drop database stadb;'
   ```

4. Load the new installation database dump file you created in Dump the New STA Database (Task 6) - Optional.

   For example:

   ```
   $ mysql -u root -p -e 'source /home/oracle/STA_FRESH_INSTALL_BACKUP.sql;'
   ```

5. Perform Upgrade the Old Database (Task 9).
6. Configure STA as a new installation. See the following sections for details:
   - Configure the Library Connection (SNMP or SCI)
   - Configure STA Services and User Information

Configure STA After the Upgrade

After upgrading, configure the libraries so that STA can continue monitoring activity

- Verify STA is Running Properly
- Update the STA Trap Recipient on the Libraries

- Configure Library Connection Settings in STA
- Configure STA Services and User Information
- Decommission the Old STA Server (optional)

Verify STA is Running Properly

Verify that all STA application services are running and active after the upgrade.

1. Open a terminal session on the STA server, and log in as the Oracle user.
2. Display the application status:

   ```
   $ STA status all
   ```

   It may take a few minutes. Once complete, you should see:

   ```
   .... and the deployed application for staui is in an ACTIVE state
   ```

3. If there are any issues with the STA services, you can review the installation and STA logs for more information. See Logs Created During Installation, Upgrade, and Deinstallation for their locations.
4. If necessary, stop and restart all STA services. It may take several minutes for the commands to complete.

   ```
   $ STA stop all
   $ STA start all
   ```

Update the STA Trap Recipient on the Libraries

Trap levels 13 (Test Trap) and 14 (Health Trap) were introduced in STA 2.0. If using the two-server method or upgrading from 1.0.x using the single-server method, you must add the new trap levels in the trap recipient definition.

Proceed as follows depending on your upgrade path:

- If you are using the two-server upgrade method, add the new STA server as a trap recipient on each monitored library, and be sure to include the new trap levels in the definition.
- If you are using the single-server method to upgrade from STA 2.0.x or later, the STA trap recipient and new trap levels are already defined on each monitored library, so you do not need to make any additional modifications. Proceed to Configure Library Connection Settings in STA.
- If you are using the single-server method to upgrade from STA 1.0.x, the STA trap recipient is already defined on each monitored library, but you must add the new trap levels to the definition. Use the appropriate steps for each library model.

SL500, SL3000, SL8500

For these library models, to modify a trap recipient, you must delete the existing definition and then add a new one.

1. Log in to the library CLI.
2. Display all existing trap recipients, and note the index number of the STA recipient.

   ```
   $ snmp listTrapRecipients
   ```

3. Delete the STA trap recipient.

   ```
   $ snmp deleteTrapRecipient id <index number of STA trap recipient>
   ```

4. Re-add the STA trap recipient and include the new trap levels in the trap level list. See Create the STA SNMP v3 Trap Recipient or Create the STA SNMP v2c Trap Recipient for instructions.

SL150

1. Log in to the browser-based user interface.
2. From the **SNMP** menu, select **SNMP Trap Recipients**.
3. Select the STA trap recipient from the list.
4. Select **Modify Trap Recipient**.
5. Add the new trap levels to the trap level list, and then click **Save**.

Configure Library Connection Settings in STA

Reconfigure the SNMP or SCI connection to the libraries to send data to the upgraded version of STA.

1. Log in to the STA GUI as an administrator user.
2. Reenter the configuration settings, using the values you recorded before the upgrade. The values must match what is configured on the monitored libraries.
3. Reconfigure the connection to each library you want STA to monitor.

   See Configure the Library Connection (SNMP or SCI) for instructions.

   For SNMP, make sure to reenter the configuration settings for the STA SNMP client, using the values you recorded before the upgrade. The values must match what is configured on the monitored libraries.
4. Restore communication between STA and the libraries by testing the connection to each monitored library.

   See Test the Library Connection.

   > **Note:**
   >
   > Once this step has completed successfully, STA begins receiving and processing data from each monitored library. You may notice incomplete exchanges on the Exchanges Overview screen from exchanges in process either when STA was stopped or when the library connections were restored. See the *STA User's Guide* for details about incomplete exchanges.

5. Get the latest SNMP library configuration data from each library.

   See Manually Collect Library Data.

Configure STA Services and User Information

Configure the STA services and re-establish the user configuration. If you want to retain settings from the previous STA version, use the values you recorded before the upgrade.

Refer to the *STA Administration Guide* to:

- Configure the Backup service
- Configure the Resource Monitor service

Refer to the *STA User's Guide* to:

- Create STA usernames and passwords. You may also want to do the following:
  - Notify users of any new password requirements.
  - Direct users to reenter their custom user preferences, if applicable.
- Configure the email server. Add email account usernames and passwords.
- Restore original ownership to custom templates.
- Restore original ownership to private Executive Report policies.
- Restore original ownership to logical groups by recreating the groups.

Decommission the Old STA Server (optional)

If you used the two-server post-installation upgrade method, you can decommission the old STA server after verifying that the new STA server is functioning as expected.

1. Remove the old STA server as a trap recipient from each library's SNMP configuration. See Delete or Modify the STA Trap Recipient.
2. Decommission the old STA server.

8
Deinstall and Restore STA

Deinstall STA to remove the STA application, all associated data, and associated Oracle software. After deinstallation, reinstall STA and restore the database to repair a current installation.

> **Caution:**
>
> You cannot downgrade STA to a previous version. Database data created with a newer version of STA will be lost when installing an older version of STA.

Create an RDA Log Bundle

Perform an RDA log snapshot on the current STA installation. Oracle Support can use the generated service logs to troubleshoot issues.

1. Log on to the STA server as the Oracle user.
2. Change to the RDA directory. For example:

   ```
   # cd /Oracle/Middleware/rda
   ```

3. Verify that the RDA `output.cfg` file is present.

   ```
   $ ls -la output.cfg
   -rw-r-----  1 oracle oinstall 23550 Mar 29 12:47 output.cfg
   ```

4. Enter the following command to generate the log bundle.

   ```
   $ ./rda.sh -f -v
   ```

   Where:

   - `-v`–Displays the progress of the data collection; this parameter is optional.
   - `-f`–Forces a current data collection.

   The utility generates an RDA log bundle with the default name `RDA_ouput_us.zip`. This may take several minutes.

5. Use any of the following commands to display information about the `rda.sh` utility:

   - **`./rda.sh -M`** —Displays the complete man page for the utility.
   - **`./rda.sh -M STA`** —Displays a summary of the log files generated by the utility for STA.

- **./rda.sh -h** —Displays help information for all utility options.

6. Rename the RDA zip file to a unique name. For example:

```
# mv RDA_output_us.zip RDA.STA_myserver_170223.zip
```

7. Optionally, use one of the following methods to display a listing of the files.
   - Open a browser window on the STA server and navigate to the URL: `file:///Oracle/Middleware/rda/output/RDA__start.htm`
   - Download the zip file to your local computer, unzip the bundle, and access the log files through the URL above.

Dump the Database

Dump the database before deinstalling STA. You can use the database dump to restore the data after reinstallation.

1. On the STA server, open a terminal session. Log in as the Oracle user.
2. Stop all STA services:

```
$ STA stop all
```

3. Start the MySQL service:

```
$ STA start mysql
```

4. Create a backup file.

```
$ /usr/bin/mysqldump -u root -p --opt --routines --triggers --events --flush-logs --single-transaction --complete-insert --comments --dump-date --add-drop-database --databases stadb -v > /<sta_db_backup>/<backup_filename>.sql

Enter password: mysql_root_password
```

Output will be similar to the following:

```
...
-- Retrieving view structure for table v_mdv_request_states...
-- Retrieving view structure for table version_info...
...
-- Disconnecting from localhost...
```

> **Note:**
>
> If you see "Can't connect to local MySQL server," the MySQL server is not running. Verify you have started MySQL.

Deinstall STA

Deinstall STA to remove the STA application, all associated data, and associated Oracle software from the server.

1. If you plan to reinstall STA, make sure you have completed the following before proceeding:
   - Create an RDA Log Bundle

- Dump the Database

2. Move the service log snapshot and database snapshot to another server, as all STA files will be removed in the next steps.

   The snapshots are located in the following directories:

   - If you created the RDA log using the GUI, the service log snapshot is in `/Oracle_storage_home/Middleware/rda/snapshots`. For example, `/Oracle/Middleware/rda/snapshots`
   - If you created the RDA log using the command line, the service log snapshot is in `/Oracle_storage_home/Middleware/rda`. For example, `/Oracle/Middleware/rda`
   - The database snapshot is in the database location specified during STA installation. For example, `/dbbackup`

3. Back up other files as needed.
4. On the STA server, open a terminal session. Log in as the Oracle user that is a member of the Oracle group. You cannot deinstall STA as the Linux `root` user nor any other user with superuser privileges.
5. Change to the installer binary directory with the STA home directory. For example:

   ```
   $ cd /Oracle/StorageTek_Tape_Analytics/oui/bin
   ```

6. Select either the wizard or silent mode to deinstall STA. Use the following commands to launch the deinstallation.

   - **Wizard:**

     ```
     $ ./deinstall.sh
     ```

     After launching the wizard, see Deinstall Using the Wizard. This mode requires an X11 display. See Installation Wizard Display Requirements for instructions.

   - **Silent-mode:**

     Before running silent mode, you must create a response file. See Create a Response File.

     ```
     $ ./deinstall.sh -silent -responseFile <absolute path to responsefile>
     ```

7. After completing the wizard or silent-mode deinstaller, verify the deinstallation was successful by listing the contents of the Oracle storage home directory. It should be empty.

   For example:

   ```
   $ ls -la /Oracle
   total 8
   drwxr-xr-x   2 oracle oinstall 4096 Sep 23 14:55 .
   dr-xr-xr-x. 31 root   root     4096 Sep 23 16:41 ..
   $
   ```

What Occurs During the Deinstallation

The STA deinstallation performs specific tasks to remove the application.

- The following subdirectories within the Oracle storage home location are removed completely. Other subdirectories are not affected.

  - `StorageTek_Tape_Analytics`—Contains all files and binaries required for the STA application.
  - `Middleware` —Contains all files and binaries required for MySQL and WebLogic.
- All STA and MySQL logs are removed from the logs location.

  See Review the STA File System Layout for details about this location.
- All STA service logs are removed except for those in `/var/log/tbi`.
- The STA database (MySQL) and all local backups are removed. If the database directory or the local backups directory are mount points or include user-defined files, the directories are retained; otherwise, they are removed.

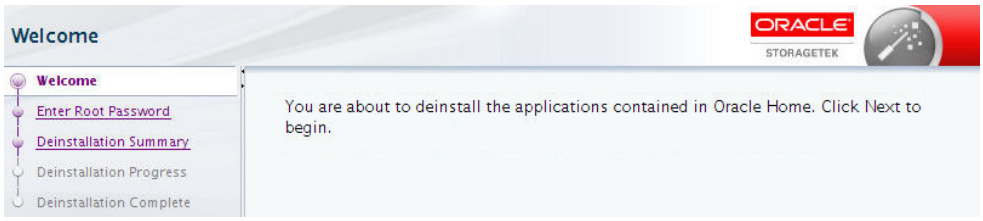
The Oracle central inventory location is *not* removed by STA deinstallation. All data in this directory is retained, including all STA installation and deinstallation logs and Oracle software inventory information.

See Oracle central inventory location and Logs Created During Installation, Upgrade, and Deinstallation.

Deinstall Using the Wizard

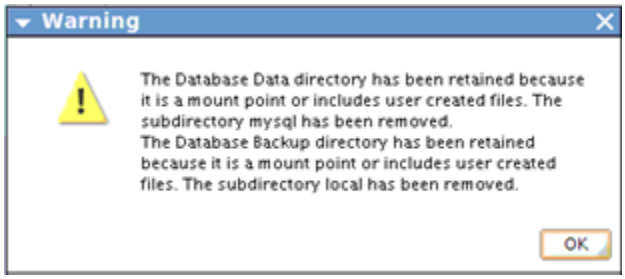
Follow the prompts of the wizard to deinstall STA.

1. Complete the steps in Deinstall STA to launch the wizard.
2. Review the *Welcome* screen, then click **Next**.



3. On the *Enter Root Password* screen, enter the existing system root password.
4. On the *Deinstallation Summary* screen, review the information, and then click **Deinstall**.
5. The *Deinstallation Progress* screen will display the current status of the deinstallation.

   IMPORTANT: Do not close this window or otherwise interrupt the deinstallation while it is in progress, as this may leave incomplete installation components on the server.
6. If either of the database locations are mount points on the STA server, the following message is displayed, notifying you that the mount point has been retained. Click **OK** to dismiss the message.



7. Once the *Deinstallation Complete* screen displays, click **Finish**.

Restore STA

Reinstall STA and restore the database to repair a current installation. You cannot use the STA installer to reinstall or overwrite a current installation, you must first deinstall the current version of STA and then reinstall STA.

1. Make sure you have removed STA from the server.

   See Deinstall STA.

2. Reinstall STA as if it were a new installation.

   See Install STA.

3. On the STA server, open a terminal session. Log in as the Oracle user.

4. Stop all STA services:

   ```
   $ STA stop all
   ```

5. Transfer the database dump.

   ```
   $ scp -p <backup_host>:/<path_to_dump_file>/<dump_name> /<local_path>
   ```

   For example, the dump file `Jan26_dump.sql.gz` is transferred from `/dbdumpfiles` on host `backup1` to the `/home/oracle` folder on the STA 2.3.1 server.

   ```
   $ scp -p backup1:/dbdumpfiles/Jan26_dump.sql.gz /home/oracle
   ```

6. Perform a checksum of the transferred file. Verify the checksum value matches the one you received when creating the database dump.

   ```
   $ cd /home/oracle/
   $ cksum <dump_name>
   ```

7. Decompress the backup file.

   ```
   $ unzip <dump_name>
   ```

8. Start the MySQL server:

   ```
   $ STA start mysql
   ```

9. Ensure there is no residual STA database (stadb) on the server. For example:

   ```
   $ mysql –u root –p –e 'drop database stadb;'
   ```

10. Load the old STA database (do not use the -v (verbose) option). Enter the database root user password when prompted. There is no command output as the process runs.

    ```
    $ mysql -u root -p -e 'source /<path_to_dump_file>/<dump_name>;'
    ```

If the command is successful, you are returned to the command prompt once the process completes.

11. Start all STA services: **`$ STA start all`**
12. Configure STA.

    See Configure Library Connection Settings in STA and Configure STA Services and User Information.

A
Installation Wizard

The installation wizard steps you through installing or deinstalling STA.

For procedures to use the wizard, see:

- Install STA with the Installation Wizard
- Deinstall Using the Wizard

The following provide information for troubleshooting issues with the wizard:

- Installation Wizard Display Requirements
- Troubleshoot Installation Wizard Display Issues

Installation Wizard Display Requirements

The wizard requires X Window System, version 11 (X11). The X11 service must be running on the STA server and configured to allow X11 forwarding.

X11 configuration is outside the scope of this guide, contact your system administrator.

If Linux was installed as instructed in Install and Configure Linux on the STA Server X11 should already be configured properly. However, you may need to set X11 authorizations and display correctly for the Oracle user. The procedures for this depend on the type of connection to the STA server.

- Set DISPLAY Variable for Direct Connections
- Set X11 for Remote Connections Using a Secure Shell (SSH)

Set DISPLAY Variable for Direct Connections

For direct connections to the STA server, you must log in as the Oracle user and then set the `DISPLAY` variable manually.

For example:

```
$ export DISPLAY=hostname:0.0
```

You may also need to verify that the Oracle user has the proper X11 authorization. Contact your Linux administrator for assistance.

Set X11 for Remote Connections Using a Secure Shell (SSH)

If you use a secure shell (SSH) with X11 forwarding enabled, the STA server automatically sets up the proper X11 authorization and display for the login user.

Enable X11 Forwarding on Linux

To enable X11 forwarding on a Linux machine, use the `ssh` command with the `-X` or `-Y` options. For example:

```
$ ssh -X oracle@sta_server
```

Enable X11 Forwarding on Windows

Your PC must be running an X11 server, such as Xming or Cygwin/X, and an SSH client, such as PuTTY or WinSCP.

1. Verify that the X11 server is running on your PC. Contact your system administrator for assistance, if necessary.
2. Start PuTTY, in the main Session window, make the following entries
   - In the **Host Name** field, type the name or IP address of the STA server.
   - In the **SSH Connection type** field, select **SSH**.
3. In the Category menu tree, expand **Connection**, then expand **SSH**, then select **X11**. In this window, make the following selections:
   - In the **X11 forwarding** field, select the **Enable X11 forwarding** check box.
   - In the **Remote X11 authentication protocol** field, select **MIT-Magic-Cookie-1**.
   - Leave the other fields blank.

Example A-1 Manually Enable the DISPLAY Variable If Not Logged In as the Oracle User

If you log in as `oracle`, the SSH service on the STA server automatically sets up the proper X11 authorization and display for the `oracle` user. You should not need to set the `DISPLAY` variable manually.

However, if you log in as a different user (for example `root`) and then `su` to `oracle`, the X11 authorizations and display will not be set correctly for the `oracle` user and you must set them manually. Instructions for doing this are outside the scope of this guide; contact your Linux administrator for assistance.

Troubleshoot Installation Wizard Display Issues

The STA installer verifies that X11 is properly configured for the Oracle user. If these prerequisite checks fail, contact your Linux system administrator for assistance.

You can use the following steps to help troubleshoot display problems.

1. Log in to the STA server as the Oracle user, and display the currently installed RPM packages.

   ```
   $ yum list installed
   ```

   The `xorg-x11-util` entry should be included in the displayed list. For example:

   ```
   xorg-x11-utils.x86_64                  7.5-6.el6
   ```

2. Display the current display settings. For example: **`$ echo $DISPLAY`**
3. Verify the display has the proper X11 configuration. For example:

   ```
   $ xdpyinfo -display :0.0
   ```

   Example showing properly configured X11:

```
$ xdpyinfo
name of display:    :0.0
version number:    11.0
vendor string:    The X.Org Foundation
vendor release number:    11300000
X.Org version: 1.13.0
maximum request size:  16777212 bytes
motion buffer size:  256
```

Example showing improperly configured X11.

```
$ xdpyinfo
xdpyinfo:  unable to open display ":0.0".

$ xdpyinfo
PuTTY X11 proxy: MIT-MAGIC-COOKIE-1 data did not matchxdpyinfo:  unable to open
display ":0.0".
```

B

Silent-mode Installer

Use the silent-mode installer to bypass the graphical installer interface and supply the installation or deinstallation input with a text file called the *response file*. This mode is useful for unattended installations and for installing STA on multiple machines.

> **Note:**
>
> Always create a new response file when installing a new version of STA. Do not reuse response files created with an older version of STA as there may be changes to format or parameters.

By using a response file, you can supply a single set of parameters to automate the installation or deinstallation process. You can run silent-mode either from a script or from the Linux command line.

Silent-mode Requirements

Before running silent-mode, verify your system meets all requirements.

Make sure you have done the following:

- Identify or Create Information Required for the Installation
- Verify Installation Prerequisites
- Download the STA Installer —the Response File Build Utility is part of the installation package.

Additional requirements include:

- A version of Java running on the server.
- You can use silent mode from telnet clients such as PuTTY, which do not use the X11 protocol. The `xorg-x11-utils` RPM package must be installed on the STA server, however.
- Silent mode also requires a central inventory pointer file specifying the location of the Oracle central inventory directory and the Oracle group. You must create the file manually if it does not exist already.

Create a Response File

The response file provides installation parameters for the silent-mode installer. Use the Response File Build Utility to create the file.

Start the Response File Build Utility

The Response File Build Utility creates the response file that provides installation values used by the silent-mode installer.

1. On the STA server, open a terminal session. Log in as the Oracle user.
2. Verify that the Oracle user has write privileges to the directory where you want to save the response file. For example:

```
$ ls -ld /home/oracle/ResponseFiles/
drwxr-xr-x 2 oracle oinstall 4096 Sep 16  2015 /home/oracle/ResponseFiles/
```

3. If you are creating a new response file, determine whether the directory includes any response files you want to keep and save them as necessary. Existing files with the default response file name will be overwritten by the response file build utility.

   The default response file names are as follows.

   - `silentInstall.rsp`—Silent installation response file
   - `silentDeinstall.rsp`—Silent deinstallation response file

   For example:

```
$ cd /home/oracle/ResponseFiles
$ ls -l *.rsp
-rw-r--r--   1 oracle   oracle          2836 Jun 30 16:49 silentInstall.rsp

$ mv silentInstall.rsp silentInstall_save.rsp
```

4. Change to the directory where you have downloaded the STA installer files. For example:

```
$ cd /Installers
```

5. Launch the response file build utility. For example:

```
$ java -jar silentInstallUtility_2.3.1.jar
```

   The utility starts and the Main Menu appears.

```
1) Create a new response file (with system prompt).
2) Create an empty response file.
```

```
3) Enter and encrypt passwords.
4) Exit.
```

6. Select an option:
   - Enter 1 and proceed to Create a Response File With Values.
   - Enter 2 and proceed to Create an Empty Response File and Manually Add Values.
   - Enter 3 and proceed to Add Encrypted Passwords to a Response File.

Create a Response File With Values

Create a response file containing all information needed to run the silent-mode installer.

1. Complete the steps in Start the Response File Build Utility, selecting 1 in the main menu of the utility.
2. Select the type of response file to create.

```
1) Silent Install
2) Silent Deinstall
```

3. Follow the prompts to input the response file values

   See Response File Parameters for descriptions of the input.

> **Note:**
>
> The response file build utility does not verify your entries. If the values do not meet the requirements, the silent-mode may fail.

4. Once you have entered all the required information, the utility creates the response file and displays its contents. The utility encrypts all passwords values.
5. You can use the response file right away with the silent-mode installer or deinstaller.

   See Run Silent-Mode to Install STA or Run Silent-Mode to Deinstall STA.

Create an Empty Response File and Manually Add Values

Create a response file with placeholders for required values. Then, add the values to the response file before running the installer.

1. Complete the steps in Start the Response File Build Utility, selecting 2 in the main menu of the utility.
2. Select the type of response file to create.

```
1) Silent Install
2) Silent Deinstall
```

3. When prompted, specify an absolute path for the directory for saving the response files or press `Enter` to use the default.
4. Use a text editor to edit the response file and provide values for all non-password parameters. See Response File Parameters. Entries must meet the parameter requirements or the silent-mode will fail.

   IMPORTANT: Do not add or modify any passwords. You must use the utility to create encrypted password values.

5. Proceed to Add Encrypted Passwords to a Response File to add the passwords to the response file.

Add Encrypted Passwords to a Response File

Add encrypted passwords to a previously used response file or on an empty file. Once a response file has been used, you cannot reuse the file until you reenter the encrypted passwords with the utility.

1. Complete the steps in Start the Response File Build Utility, selecting 3 in the main menu of the utility.
2. Select the type of response file to update.

```
1) Silent Install
2) Silent Deinstall
```

3. Enter the absolute path of the response file you want to update, including the file name.

   The utility prompts for your input. The prompts vary based on the type of response file you have selected.
4. Respond to each prompt to enter the password parameters. The values are not shown on screen.

   The utility adds the encrypted passwords to the response file and displays the file contents.
5. Exit the utility. Use the response file with the silent-mode installer or deinstaller.

   See Run Silent-Mode to Install STA or Run Silent-Mode to Deinstall STA.

Response File Parameters

The response file parameters are used by the silent-mode installer to input configuration values.

Table B-1 Response File Reference

Response File Build Utility Prompt	Parameter	Description
`Enter location where STA will be installed (STORAGE_HOME)`	`STORAGE_HOME`	Absolute path where STA will be installed. The Oracle user and group must have the following permissions: • If the directory already exists, they must have full permissions to it. • If the directory does not exist, they must have full permissions to the parent directory, so the STA installer can create the Oracle Storage Home directory.
`Enter the System Root password`	`ROOT_ACCESS_PASSWORD`	Password for the existing system root user.
`Enter location for Database Data directory`	`DBDATA_LOC`	Absolute path to the directory where the STA database will be located.

Table B-1 (Cont.) Response File Reference

Response File Build Utility Prompt	Parameter	Description
Enter location for Database Backup directory	DBBACKUP_LOC	Absolute path to the directory where the STA database backups will be located. This cannot be the same as the database data location.
Enter Weblogic Administrator Username	WEBLOGIC_ADMIN_NAME	User for logging into the WebLogic administration console.
Enter Weblogic Administrator Password	WEBLOGIC_ADMIN_PASSWORD	Password for WebLogic user. Modify with response file build utility only.
Enter STA Administrator Username	STAGUI_ADMIN_NAME	User for logging into the STA user interface.
Enter STA Administrator Password	STAGUI_ADMIN_PASSWORD	Password for STA Admin user. Modify with response file build utility only.
Enter STA Database Root User Password	MYSQL_ROOT_PASSWORD	Password for the account used internally by the STA application to create the database. The username is automatically set to root. Modify with response file build utility only.
Enter STA Database Application Username	MYSQL_APP_NAME	MySQL account used internally by the STA application to connect to and update the STA database.
Enter STA Database Application Password	MYSQL_APP_PASSWORD	Password for database application user. Modify with response file build utility only.
Enter STA Database Reports Username	MYSQL_RPTS_NAME	MySQL account used by non-STA and third-party applications to connect to the STA database.
Enter STA Database Reports Password	MYSQL_RPTS_PASSWORD	Password for Database Reports user. Modify with response file build utility only.
Enter STA Database Administrator Username	MYSQL_DBA_NAME	MySQL account used internally by STA utilities to connect to the STA database and configure and run scheduled backups.
Enter STA Database Administrator Password	MYSQL_DBA_PASSWORD	Password for the Database Administrator user. Modify with response file build utility only.
Enter WebLogic Administration Console HTTP Port Enter WebLogic Administration Console HTTPS Port	ADMINSERVER_HTTP_PORT ADMIFNSERVER_HTTPS_PORT	See Ports Configured During STA Installation for typical values used.
Enter staEngine HTTP port Enter staEngine HTTPS port	STAENGINE_HTTP_PORT STAENGINE_HTTPS_PORT	See Ports Configured During STA Installation for typical values used.
Enter staAdapter HTTP port Enter staAdapter HTTPS port	STAADAPTER_HTTP_PORT STAADAPTER_HTTPS_PORT	See Ports Configured During STA Installation for typical values used.
Enter staUi HTTP port Enter staUi HTTPS port	STAUI_HTTP_PORT STAUI_HTTPS_PORT	See Ports Configured During STA Installation for typical values used.

Table B-1 (Cont.) Response File Reference

Response File Build Utility Prompt	Parameter	Description
Enter SNMP Trap Redirection Port	SNMPTRAP_PORT	In STA 2.3.0+, this is the internal port where SNMP notifications (traps) are redirected. See Ports Configured During STA Installation for typical values used.
Enter RDA domain name	DOMAIN_NAME	Your site's fully qualified domain name. For example, us.example.com..
None	KEYFILE_LOC	Location of password encryption key file. Do not modify; automatically generated by response file build utility.
None	ORACLE_HOME	Subdirectory within Storage Home where STA will be installed. Do not modify; automatically generated by response file build utility.

Sample Response Files

Sample response files can help give you an idea of how to configure your response file.

Example B-1 Sample Install Response File With Values

```
[ENGINE]

# DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0

[GENERIC]

# Location of the Key file used to secure the passwords.
KEYFILE_LOC=/Installers/.sk1443551626070

# The oracle home location. This can be an existing or new Oracle Home. The
directory should end with StorageTek_Tape_Analytics
ORACLE_HOME=/Oracle/StorageTek_Tape_Analytics

# The Storage Home location. This can be an existing or new Storage Home.
STORAGE_HOME=/Oracle

# System Root Password. This needs to be encrypted using the SilentInstallUtility
ROOT ACCESS PASSWORD=zoz33BM5C1U92DHZLxTjVw==

# Confirm System Root Password. This needs to be encrypted using the
SilentInstallUtility
ROOT ACCESS CONFIRM PASSWORD=zoz33BM5C1U92DHZLxTjVw==

# Directory for DB Data
DBDATA LOC=

# Directory for DB Backup
DBBACKUP LOC=
```

```
# Weblogic Administrator Username
WEBLOGIC ADMIN NAME=

# Weblogic Administrator Password. This needs to be encrypted using the
SilentInstallUtility
WEBLOGIC ADMIN PASSWORD=Ys+zaD3ZY44wwX3cwfbzTw==

# Confirm Weblogic Administrator password. This needs to be encrypted using the
SilentInstallUtility
WEBLOGIC ADMIN CONFIRMPASSWORD=Ys+zaD3ZY44wwX3cwfbzTw==

# STA GUI Administrator username
STAGUI ADMIN NAME=

# STA GUI Administrator password. This needs to be encrypted using the
SilentInstallUtility
STAGUI ADMIN PASSWORD=6wlTC2NyshF9T0gJ+pwLUQ==

# Confirm STA GUI Administrator password. This needs to be encrypted using the
SilentInstallUtility
STAGUI ADMIN CONFIRMPASSWORD=6wlTC2NyshF9T0gJ+pwLUQ==

# Enter STA Database Root User password. This needs to be encrypted using the
SilentInstallUtility
MYSQL ROOT PASSWORD=6wlTC2NyshF9T0gJ+pwLUQ==

# Confirm STA Database Root User password. This needs to be encrypted using the
SilentInstallUtility
MYSQL ROOT CONFIRM PASSWORD=6wlTC2NyshF9T0gJ+pwLUQ==

# STA Database Application User
MYSQL APP NAME=

# STA Database Application Password
MYSQL APP PASSWORD=6wlTC2NyshF9T0gJ+pwLUQ==

# Confirm STA Database Application Password
MYSQL APP CONFIRMPASSWORD=6wlTC2NyshF9T0gJ+pwLUQ==

# STA Database Reports user
MYSQL RPTS NAME=

# STA Database Reports Password
MYSQL RPTS PASSWORD=6wlTC2NyshF9T0gJ+pwLUQ==

# Confirm STA Database Reports Password
MYSQL RPTS CONFIRMPASSWORD=6wlTC2NyshF9T0gJ+pwLUQ==

# STA Database Administrator
MYSQL DBA NAME=

# STA Database Administrator password
MYSQL DBA PASSWORD=6wlTC2NyshF9T0gJ+pwLUQ==

# Confirm STA Database Administrator password
MYSQL DBA CONFIRMPASSWORD=6wlTC2NyshF9T0gJ+pwLUQ==

# WebLogic Administration Console HTTP Port
ADMINSERVER HTTP PORT=

# WebLogic Administration Console HTTPS Port
```

```
ADMINSERVER HTTPS PORT=

# STA Engine HTTP Port
STAENGINE HTTP PORT=

# STA Engine HTTPS port
STAENGINE HTTPS PORT=

# STA Adapter HTTP Port
STAADAPTER HTTP PORT=

# STA Adapter HTTPS Port
STAADAPTER HTTPS PORT=

# STA UI HTTP Port
STAUI HTTP PORT=

# STA UI HTTPS Port
STAUI HTTPS PORT=

#SNMPTrap Port
SNMPTRAP PORT=

# RDA Domain Name
DOMAIN NAME=
```

Example B-2 Sample Deinstall Response File With Values

```
[ENGINE]

# DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0

[GENERIC]

# Location of the Key file used to secure the passwords.
KEYFILE_LOC=/Installers/.sk1589225815277

# This will be blank when there is nothing to be de-installed in distribution
level
SELECTED_DISTRIBUTION=STA_Install~2.3.1.0.0

# System Root Password. This needs to be encrypted using the SilentInstallUtility
DEINSTALL ROOT ACCESS PASSWORD=S8+aD4n7qOwOKOUTApcKZg==

# Confirm System Root Password. This needs to be encrypted using the
SilentInstallUtility
DDEINSTALL ROOT ACCESS CONFIRM PASSWORD=S8+aD4n7qOwOKOUTApcKZg==
```

Run Silent-Mode to Install STA

Silent-mode uses a response file to provide input for the installation. This mode is useful for unattended installations and for installing STA on multiple machines.

1. Before running the installer, you must configure a response file.

   See Create a Response File.
2. On the STA server, open a terminal window. Log in as the Oracle user.
3. Change to the STA installer location. For example:

```
$ cd /Installers
```

4. Start the STA silent-mode installer.

   See Installer Command Options for full definitions of the command parameters.

   ```
   $ ./sta_installer_linux64_<version>.bin -silent  -responseFile <absolute path to
   response file> -invPtrLoc <absolute path to Oracle central inventory pointer file>
   ```

   For example:

   ```
   $ ./sta_install_2.3.1_linux64.bin -silent -responseFile /Installers/
   silentInstall.rsp -invPtrLoc /Oracle/oraInventory/oraInst.loc
   ```

5. The installer displays status messages in the terminal window as it performs the following installation steps. This process may take 30 to 60 minutes to complete.

   - Performs prerequisite checks on the STA server environment.
   - Verifies that the response file is valid and includes entries for all required parameters.
   - Installs the included software packages, including MySQL, WebLogic, and the STA application.
   - Configures the STA environment using the settings you have supplied in the response file.
   - Starts the STA application.

   If successful, you should see:

   ```
   Configuration:Post Configuration completed successfully
   The installation of STA_Install 2.3.1 completed successfully.
   Logs successfully copied to /Oracle/StorageTek_Tape_Analytics/cfgtoollogs/oui.
   ```

   If it fails, you may see:

   ```
   [ERROR] Rule_CalculateFreeSpace_Error. Aborting Install
   Logs are located here: /tmp/OraInstall2016-09-24_09-29-29AM.
   ** Error during execution, error code = 256.
   ```

6. When the installer completes successfully, verify that STA is running.

   See Verify Successful Installation for instructions.

Run Silent-Mode to Deinstall STA

Deinstall the current version of STA using the silent-mode deinstaller.

1. Before running the installer, you must configure a response file.

   See Create a Response File.

2. On the STA server, open a terminal window. Log in as the Oracle user.
3. Change to the STA home directory. For example:

   ```
   $ cd /Oracle/StorageTek_Tape_Analytics
   ```

4. Change to the STA utilities directory.

   ```
   $ cd oui/bin
   ```

5. Start the STA silent-mode deinstaller.

   ```
   $ ./deinstall.sh -silent  -responseFile <absolute path to response file> -
   invPtrLoc <absolute path to Oracle central inventory pointer file>
   ```

For example:

```
$ ./deinstall.sh -silent  -responseFile /Installers/SilentDeinst.rsp -invPtrLoc /Oracle/
oraInventory/oraInst.loc
```

See Installer Command Options for full definitions of available parameters.

6. The deinstaller displays status messages in the terminal window as it deinstalls the STA application and data, MySQL, and WebLogic. This process may take up to 30 minutes to complete.

   See What Occurs During the Deinstallation for details about the updates made.

   If successful, you should see:

   ```
   The uninstall of STA_Install 2.2.0.0.0 completed successfully.
   Logs successfully copied to /home/oracle/oraInventory/logs.
   ```

   If it fails, you may see:

   ```
   Internal Error: File Copy failed. Aborting Install
   Logs are located here: /tmp/OraInstall2016-09-25_10-07-18AM.
   ```

7. Verify the deinstallation was successful by listing the contents of the Oracle storage home directory. It should be empty. For example:

   ```
   $ ls -la /Oracle
   total 8
   drwxr-xr-x   2 oracle oinstall 4096 Sep 23 14:55 .
   dr-xr-xr-x. 31 root   root     4096 Sep 23 16:41 ..
   $
   ```

Installer Command Options

You specify installer command options when launching the installer. Some options only apply to the silent-mode installer.

Table B-2 Installer Command Options

Option	Description	Applies to:
-force	Allow silent-mode installation into a non-empty directory.	Silent-mode only
-invPtrLoc *pointer_file*	This parameter is required only if there is no `/etc/oraInst.loc` file or you want to use a different file. Uses the specified Oracle central inventory pointer file instead of the one located in`/etc/oraInst.loc`. `pointer_file` must be an absolute path. The contents of the Oracle central inventory file are as follows: `inventory_loc=`*`Oracle_central_inventory_location`* `inst_group=`*`Oracle_install_group`* Where: • `Oracle_central_inventory_location` is the absolute path of the Oracle central inventory. • `Oracle_install_group` is the name of the Oracle group.	Silent-mode only
-response, -responseFile *response_file*	Required for silent mode. Location of the response file containing input for the STA silent-mode installer, upgrade, or deinstaller. `response_file` must be an absolute path.	Silent-mode only

Table B-2 (Cont.) Installer Command Options

Option	Description	Applies to:
-silent	Required for silent mode. Indicates to use silent mode. Inputs are taken from the specified response file.	Silent-mode only
-debug	Logs debug information. Some debug information will also appear in the console window	Graphical and silent-mode
-logLevel *level*	Omits log messages whose priority levels are lower than the specified level. Values for `level` are: severe, warning, info, fine, finer, finest	Graphical and silent-mode
-printdiskusage	Logs debug information about disk usage.	Graphical and silent-mode
-printmemory	Logs debug information about memory usage.	Graphical and silent-mode
-printtime	Logs debug information about elapsed time.	Graphical and silent-mode
-compatibilityFile *compatibility_file*	Location of the file that specifies feature set dependency changes.	Graphical and silent-mode
-executeSysPrereqs	Executes the system environment prerequisite checks for running the installer, then exit without performing the installation.	Graphical and silent-mode
-help	Displays help.	Graphical and silent-mode
–-, -install	Use graphical mode. This is the default.	Graphical only
-J–Djava.io.tmpdir=*working_directory*	Unpack the STA installer files to the specified working directory instead of `STA_home/tmp`. `working_directory` must be an absolute path, and the directory must allow the execution of binaries. This parameter does not apply to the WebLogic installer files; they are always unpacked to `STA_home/tmp`, regardless of this setting. You should ensure that there is sufficient space in all applicable directories before beginning the installation. All STA and WebLogic installer files are deleted when the installer finishes, whether successful or not.	Graphical and silent-mode
–paramFile *initialization_file*	Use the specified initialization file instead of one located in `STA_home/oui/oraparam.ini`. `initialization_file` must be an absolute path. The STA installer uses the file you specify for all operations, including the prerequisite checks. The default location is in the `STA_home/oui` directory.	Graphical and silent-mode

C

Record Installation and Upgrade Information

Use these checklists and worksheets to plan and organize the information for an STA installation or upgrade.

See Users, Groups, and Locations Used by the STA Installer for complete details about the requested information.

If you are upgrading from a previous version of STA, you can use the "Current Value" columns in the worksheets to record the values used in your current installation. Use the "New Value" columns to record the values you will use for the new version of STA.

- Upgrade Preparation Checklist
- Record Installation Users and Locations
- Record User Accounts
- Verify Port Numbers
- Record the Domain Name
- Record the SNMP Configuration

Upgrade Preparation Checklist

Track the activities you must perform to prepare for the upgrade.

See Prepare STA for the Upgrade for complete details about these activities.

- Verify the current STA version is a released version.
- Determine if you need to install a new version of Linux.
- Choose single-server or two-server upgrade method.
- Verify site and target server meet requirements for the new version of STA.
- Determine whether you will need to temporarily increase the size of your `/tmp` file system for the upgrade.
- Review environment changes in the new version of STAor impact to your upgrade plan.
- Ensure all required RPM packages are installed.
- Verify the current version of STA has recent, successful communication with the monitored libraries.
- Verify STA is processing exchanges across all monitored libraries.
- Move installation and database logs you want to retain to a safe place (optional).
- Perform service log snapshot on current STA installation (optional).
- Download service log bundles you want to retain (optional).
- Rename custom templates with "STA–" prefix (optional).
- Record current custom template settings you want to retain (optional).

- Record Executive Report policy settings you want to retain (optional).

Record Installation Users and Locations

Track user accounts and locations used to run the STA installer.

Oracle group

Description: Linux group used for installing and upgrading Oracle products on the STA server. Introduced in STA 2.1.0.

- Current value:
- New value:

Oracle user

Description: Linux user for installing, upgrading, and administering Oracle products on the STA server. Introduced in STA 2.1.0.

- Current value:
- New value:

Oracle Central Inventory Location

Description: Directory for tracking information about Oracle products installed on the STA server. Introduced in STA 2.1.0.

- Current value:
- New value:

Oracle Storage Home Location

Description: Directory where STA and associated Oracle software are installed. Introduced in STA 2.1.0.

- Current value:
- New value:

STA installer location

Description: Location where the STA installer is downloaded.

- Current value:
- New value:

STA database data location

Description: Location of the STA database.

- Current value:
- New value:

STA database backup location

Description: Location of the STA database backups on the STA server.

- Current value:
- New value:

Record User Accounts

Track accounts used for STA administration activities, and MySQL accounts used internally by the STA application to access and manage the STA database.

WebLogic Administration

Description: Used to log in to the WebLogic Administration console.

> **Caution:**
>
> You cannot retrieve this username or password. If these credentials are lost, STA must be re-installed.

- Current credentials:
- New credentials:

STA Administrator

Description: Used to log in to the STA application with full access privileges.

- Current credentials:
- New credentials:

STA Database Root User

Description: Owns the MySQL database. The predefined username of `root` cannot be changed.

> **Caution:**
>
> You cannot retrieve this password.

- Current credentials: username = root
- New credentials: username = root

STA Database Application User

Description: STA uses this account to connect to the database.

- Current credentials:
- New credentials:

STA Database Reports User

Description: Non-STA and third-party applications use this account to connect to the database.

- Current credentials:
- New credentials:

STA Database Administrator User

Description: STA administration and monitoring utilities use this account to connect to the database, primarily to perform scheduled backups.

- Current credentials:
- New credentials:

Verify Port Numbers

Track external and internal ports used by the STA application. Verify with your network administrator that these ports are open and available.

> **Note:**
>
> Changes to the default WebLogic Administration console port numbers were introduced in STA 2.1.0.

Table C-1 Unconfigurable External Ports

Port Description	Protocol	Port
Secure Shell. Used to log in from the STA server to the STA database backup and the monitored libraries.	SSH	22
Used for transmitting Simple Network Management Protocol (SNMP) requests to the monitored libraries.	SNMP	161
Used for receiving SNMP notifications (traps) from the monitored libraries. In STA 2.3.0+, this port is redirected to the port defined in during installation (SNMP Trap Redirection Port).	SNMPTRAP	162

Table C-2 Configurable Internal and External Ports

Port Description	Type	Protocol	Default Port
Unsecure port for the WebLogic Administration console (default for STA 1.0.x and 2.0.x was 7001)	External	HTTP	7019
Secure port for the WebLogic Administration console (default for STA 1.0.x and 2.0.x was 7002)	External	HTTPS	7020
Unsecure port for the staUi managed server, which manages the STA GUI	External	HTTP	7021
Secure port for the staUi managed server	External	HTTPS	7022
Unsecure port for the staEngine managed server, which manages basic STA internals	Internal	HTTP	7023
Secure port for the staEngine managed server	Internal	HTTPS	7024
Unsecure port for the staAdapter managed server, which manages SNMP communication with the monitored libraries	Internal	HTTP	7025
Secure port for the staAdapter managed server	Internal	HTTPS	7026
SNMP Trap Redirection Port	Internal	HTTPS	7027

Record the Domain Name

Track your site's fully qualified domain name used by Oracle's Remote Diagnostic Agent (RDA) when generating STA service logs.

Company domain name (for example, us.example.com)

- Current Value:
- New Value:

Record the SNMP Configuration

Track information used to configure the SNMP connection between STA and the monitored libraries.

The same SNMP v3 user must be configured on each monitored library and STA instance. See Configure SNMP (for SL150, SL500, SL3000, SL8500) for complete details about the requested information.

SNMP v3 Username

- Current Value:
- New Value:

SNMP v3 Authorization Password (Auth)

- Current Value:
- New Value:

SNMP v3 Privacy Encryption Password (Privacy)

- Current Value:
- New Value:

SNMP v2c User Community

- Current Value:
- New Value:

SNMP v2c Trap Community

- Current Value:
- New Value:

D

Configure Security Certificates

Oracle supplies self-generated security certificates for HTTPS/SSL ports. You can optionally replace it with your own certificate from a certificate authority (for example, VeriSign).

If you want to use a different security certificate than the default, perform these procedures in the order listed.

- Establish the Initial HTTPS/SSL Connection
- Reconfigure WebLogic to use a Different Security Certificate
- Replace the Oracle Certificate

Establish the Initial HTTPS/SSL Connection

Configure the browser to accept the initial HTTPS connection.

1. In a browser, enter the HTTPS/SSL version of the URL for the STA application.

   https://*<STA_host_name>*:*<HTTPS port>***/STA/**

   For example: `https://staserver.example.com:7022/STA/`

2. Accept the security warning. Depending on your browser version, the following steps may be different. The following is for Mozilla Firefox.
   a. On the Warning screen, click **Details...**
   b. To examine the certificate, click the **View Certificate**. Then, click **Close** to return to the Add Security Certificate screen.
   c. Click **Accept the Risk and Continue**.

      The certificate is added to the STA server, and you can now use HTTPS with the certificate.

Reconfigure WebLogic to use a Different Security Certificate

Change the settings of WebLogic to replace self-signed certificate with on signed by a CA.

1. In a browser, enter the URL of the WebLogic Administrator console. The URL uses one of the following formats:

   http://<local_host_name>:<port_number>**/console**
   https://<local_host_name>:<port_number>**/console**

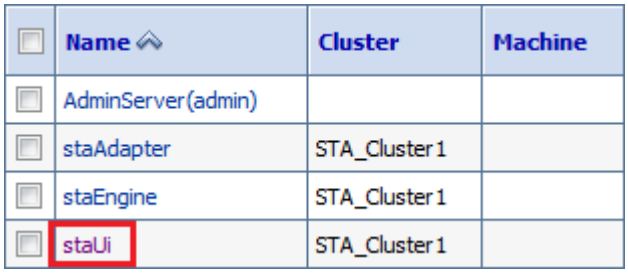
   where `local_host_name` and `port_number` are the name and port number of the WebLogic Administrator console defined during STA installation. The default HTTP port number is 7019, and the default HTTPS port number is 7020. For example:

   `https://sta_server:7020/console`

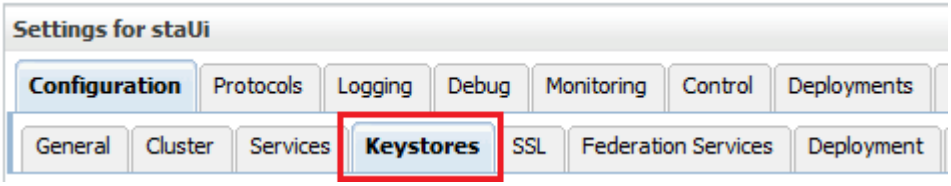
2. Enter the WebLogic Administration console username and password defined during STA installation, and then click **Login**.

3. In the Domain Structure section, select **Environment**, and then select **Servers**.

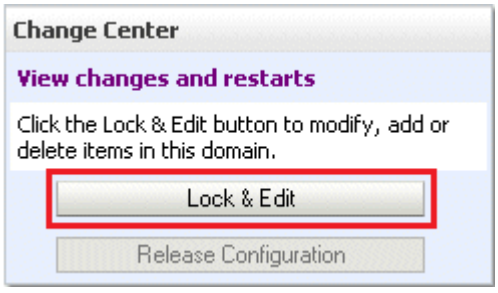
4. In the Servers table, select the **staUi** active link (not the check box).



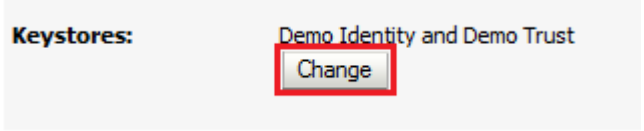
5. Select the **Keystores** tab.



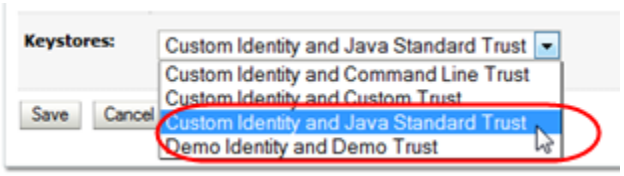
6. In the Change Center section, click **Lock & Edit**.



7. In the Keystores section, click **Change**.



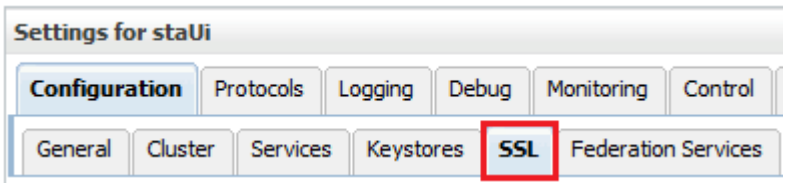
8. In the **Keystores** menu, select `Custom Identity and Java Standard Trust`.



9. Click **Save**.
10. Complete the Keystores screen as follows:
    - **Custom Identity Keystore**—Path and file of the private key file.
    - **Custom Identity Keystore Type**—Keystore type. If configuring for RACF authentication, enter `PKCS12`.
    - **Custom Identity Keystore Passphrase**—Password supplied by the MVS system administrator.
    - **Java Standard Trust Keystore Passphrase**—New password for the Java Standard Trust Keystore file.

> **Caution:**
>
> If you forget these passwords, you must reinstall STA.

11. Click **Save**.
12. Select the **SSL** tab.

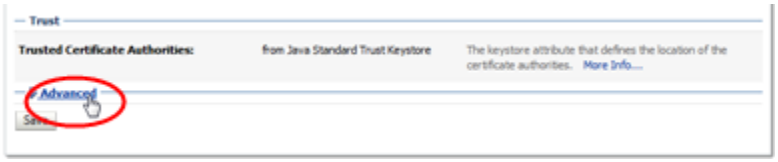


13. Enter the **Private Key Alias** and **Private Key Passphrase** supplied by the MVS system programmer.

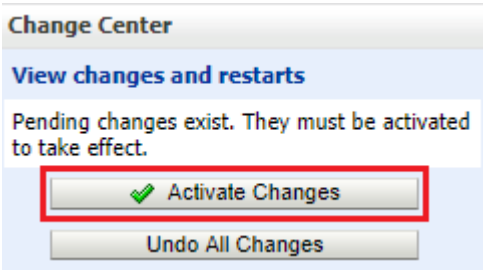
    To determine the Private Key Alias, use the `keytool` command at the system command line. For example:

```
$ keytool -list -keystore CLTBI.PKCS12DR.D080411 -storetype PKCS12
Enter keystore password: (password from the MVS sysadmin)
Keystore type: PKCS12
Keystore provider: SunJSSE

Your keystore contains 1 entry

tbiclient, Aug 17, 2011, PrivateKeyEntry,
Certificate fingerprint (MD5): 9A:F7:D1:13:AE:9E:9C:47:55:83:75:3F:11:0C:BB:46
```

14. Click **Save**.
15. In the Trusted Certificate Authorities section, click **Advanced**.



16. Complete the Advanced section of the SSL screen as follows:
    - **Use Server Certs**—Select the check box.
    - **Two Way Client Cert Behavior**—Select `Client Certs Requested But Not Enforced`.
    - **Inbound Certification Validation**—Select `Builtin SSL Validation Only`.
    - **Outbound Certificate Validation**—Select `Builtin SSL Validation Only`.
17. Click **Save**.
18. In the Change Center section, click **Activate Changes**.



19. Log out of WebLogic.
20. Stop all STA services. See the *STA Administration Guide* for command usage details.

    ```
    $ STA stop all
    ```
21. Start all STA services.

    ```
    $ STA start all
    ```

Replace the Oracle Certificate

Configure the browser to accept the new certificate.

1. Start a supported Web browser on your computer and enter the HTTPS/SSL version of the URL for the STA application.

   https://*<STA_host_name>*:*<HTTPS port>***/STA/**

   For example: `https://staserver.example.com:7022/STA/`
2. Add a security exception to have the browser accept the certificate.

E

Configure External Authentication Providers

Configure Oracle's WebLogic Server to use one or more external authentication providers to authenticate users for STA. Use the WebLogic Administration console for all STA authentication provider configuration tasks in WebLogic Server.

For most sites, the `DefaultAuthenticator` may be the only authentication provider needed for STA. You can create and maintain STA usernames through the STA user interface, and the `DefaultAuthenticator` will authenticate and authorize users as they log in. For some sites, however, it may be desirable to use external providers, in addition to the `DefaultAuthenticator`, to authenticate STA users. This is useful if your site has many users with credentials already defined on external authentication servers. You can configure one or more external authentication providers for STA.

> **Caution:**
>
> Only experienced IT administrators who have a thorough knowledge of LDAP, Microsoft Active Directory, RACF, X.500 distinguished names, and network IT Security administration should attempt making changes to STA Weblogic functionality. Incorrect or incomplete configurations can result in creating security vulnerabilities, performance issues, denial-of-service, erratic application behavior, loss of data, or STA functionality failure requiring re-installation of the STA application.

See Also:

- *Fusion Middleware Securing Oracle WebLogic Server* for complete details about managing user authentication with WebLogic Server.
- *STA User's Guide* to create users from within the STA application

Supported Authentication Provider Types

STA only supports certain authentication provider types.

- OpenLDAP
- Microsoft Active Directory (AD)
- IBM Resource Access Control Facility (RACF)

Configure SSL for Communications

If the connection between WebLogic Server and the external authentication server is to be secured through SSL, you must follow certain steps.

- Ensure that the `SSLEnabled` attribute is selected on the Provider Specific screen. See Define Provider-specific Information for instructions.
- Create and configure a custom trust keystore in WebLogic Server for use with the external authentication server. See *Fusion Middleware Securing Oracle WebLogic Server* for instructions.

Configure Active Directory and OpenLDAP Authentication Providers

To configure OpenLDAP and Microsoft Active Directory authentication providers, you must perform the tasks in the order listed.

- Prepare the External Authentication Provider for STA Authentication
- Lock the WebLogic Server Active Security Realm
- Add an External Authentication Provider
- Define Provider-specific Information
- Set the JAAS Control Flag
- Ensure Proper Order of Authentication Providers
- Apply All Configuration Changes
- Verify Configuration of Authentication Providers

Prepare the External Authentication Provider for STA Authentication

Prepare an external authentication provider to authenticate STA users. This procedure provides general guidelines only, as the specific details depend on your site configuration. Perform these steps on the external authentication server.

1. Identify or create the LDAP Principal User, which WebLogic Server will use to access the external authentication provider.
2. Create the STA Access Group. This group must have the name `StorageTapeAnalyticsUser`.
3. Identify all users needing access to STA and assign them to the STA access group.
4. Record site-specific configuration information, which you will use to configure the provider in WebLogic Server. See Define Provider-specific Information for examples of the information to gather.

LDAP Principal User

Each external authentication provider must include a user account that WebLogic Server can use to connect to the external provider. In WebLogic Sever, this user is called the *Principal* user.

You can either create a new user account or use an existing one. This user must have read and write access to the external provider's authentication directory so WebLogic Server can resolve user and group searches and authentications. This user does not need to be assigned to the STA access group.

STA Access Group

All users requiring access to STA must belong to the STA access group, which has the name `StorageTapeAnalyticsUser`. All providers performing authentication for STA must include this group.

For the `DefaultAuthenticator`, this group is created during STA installation, and all users added through the STA installer, WebLogic Administration console, and STA user interface are assigned to this group automatically.

For external authentication providers, you must create this group in the provider and assign the appropriate users to it.

Lock the WebLogic Server Active Security Realm

Lock the Security Realm to ensure no one else can make changes while you are configuring WebLogic.

1. In a browser, go to the WebLogic Administrator console. The URL uses one of the following formats:

   ```
   http://local_host_name:port_number/console
   ```

   ```
   https://local_host_name:port_number/console
   ```

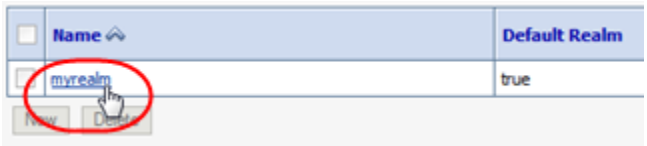
   where `local_host_name` and `port_number` are the name and port number of the WebLogic Administrator console defined during STA installation. The default HTTP port number is 7019, and the default HTTPS port number is 7020.

   For example:

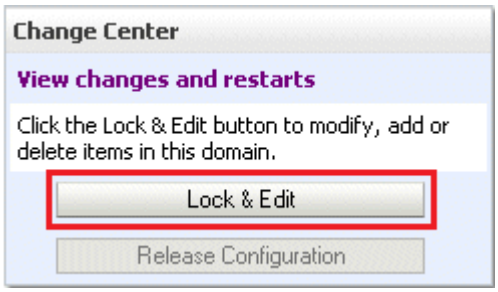
   `https://sta_server:7020/console`

2. Enter the WebLogic Administration console username and password defined during STA installation, and then click **Login**.
3. In the Domain Structure navigation tree, select **Security Realms**.

4. In the Realms table, select the **myrealm** active link.



5. In the Change Center, click **Lock & Edit**. This locks out other users from making changes at the same time.



6. Proceed to Add an External Authentication Provider .

Understand the WebLogic Server Active Security Realm

The WebLogic Server manages all user authentication for STA. All authentication providers for STA must be defined in the`myrealm` security realm.

WebLogic Server includes an embedded LDAP server, and this is the default authentication provider for STA. During STA installation, the embedded LDAP server is configured in the active security realm with the name `DefaultAuthenticator`. The `DefaultAuthenticator` data store includes credentials for the two default user accounts defined during STA installation—the WebLogic Administrator and the default STA Administrator. It also includes credentials for all STA usernames created through the STA user interface.

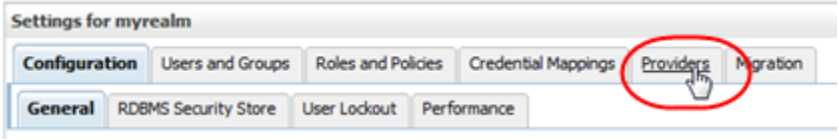
Do not change the names of the `myrealm` security realm and the `DefaultAuthenticator`; these names are required for STA.

The active security realm also includes a provider named `DefaultIdentityAsserter`. Do not make any changes to this provider.

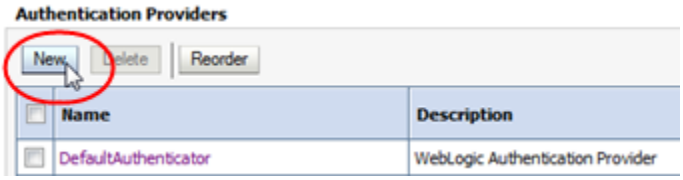
Add an External Authentication Provider

Add an external authentication provider to the WebLogic Server active security realm.

1. Make sure you have locked the active security realm from other users (see Lock the WebLogic Server Active Security Realm).
2. Within the *Settings for myrealm* section, click the **Providers** tab.



3. In the Authentication Providers table, click **New**.



4. Complete the Create a New Authentication Provider screen:
   - **Name**—Enter a name to identify the authentication provider in the WebLogic Server security realm. For example, "My External OpenLDAP Server" or "My AD Server".
   - **Type**—Select one of the following options:
     - For OpenLDAP providers, select `OpenLDAPAuthenticator`.
     - For Microsoft Active Directory providers, select `LDAPAuthenticator`.

> **Note:**
>
> The `ActiveDirectoryAuthenticator` option is not supported; do not use it, even for Microsoft Active Directory providers.

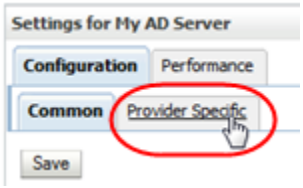
5. Proceed to Define Provider-specific Information.

Define Provider-specific Information

Define provider-specific information for each external authentication provider you have added to the WebLogic Server active security realm.

1. Make sure you have locked the active security realm from other users (see Lock the WebLogic Server Active Security Realm).
2. Make sure you have gathered the necessary configuration information from the external authentication provider (see Prepare the External Authentication Provider for STA Authentication).
3. In the Settings for myrealm control bar, select the **Providers** tab.
4. In the Authentication Providers table, select the active link for the provider you want to configure.

5. In the control bar, select the **Configuration** tab, and then the **Provider Specific**.



6. Complete the screen attributes using the values you gathered from the external authentication provider. These values must match the directory schema and other configuration attributes specific to that provider.

   Following are guidelines for attributes required for a basic configuration. Depending on your site requirements, you may need to enter values for other attributes as well.

   - **Host**—IP address of the external authentication server
   - **Port**—Port number on which the external authentication server is listening. Typically this is 389.
   - **Principal**—Distinguished Name of the user account on the external provider that WebLogic Server will use to connect to the external authentication server.
   - **Credential** and **Confirm Credential**—Password for the Principal user
   - **SSLEnabled**—Select this check box if communication between WebLogic Server and the external authentication server will be through SSL. You must perform additional configuration tasks to fully enable this feature. See Configure SSL for Communications for details.
   - **User Base DN**—Base distinguished name (DN) of the tree that contains users.
   - **User From Name Filter**—Filter WebLogic Server should use to find users
   - **User Object Class**—LDAP object class that stores users
   - **Group Base DN**—Base distinguished name (DN) of the tree that contains groups
   - **Group From Name Filter**—Filter WebLogic Server should use to find groups
   - **Group Object Class**—LDAP object class that stores groups
   - **Connection Timeout**—The default value is 0, which indicates no timeout limit. Oracle recommends setting this value to a nonzero value, such as 60 (expressed in seconds).
   - **Follow Referrals**—Select this check box if the external authentication provider is configured to use referrals to other authentication servers. If an external authentication provider uses LDAP referrals, you must ensure that the `Follow Referrals` attribute is selected on the Provider Specific screen This attribute is selected by default, but Oracle recommends y

7. When you have finished entering screen values, click **Save**. Proceed to Set the JAAS Control Flag.

   The following examples show sample values for an OpenLDAP and a Microsoft Active Directory provider, respectively. The values you enter will be different, but these examples may assist you.

Example E-1 Sample Provider-specific Values for an OpenLDAP Provider

```
Host: 10.123.456.789
Port: 389
Principle: cn=root,o=staOpen,dc=mycompany,dc=com
Credential: OpenLDAP root password>
Confirm credential:  OpenLDAP root password
SSL Enable: not selected
User Base DN:  ou=users,o=staOpen,dc=mycompany,dc=com
All Users Filter:
User From Name Filter: (&(cn=%u)(objectclass=posixAccount))
User Search Scope:  subtree
User Name Attribute:  cn
User Object Class:  posixAccount
Use Retrieve User Name as Principle:  selected
Group Base DN:  ou=groups,o=staOpen,dc=mycompany,dc=com
All Groups Filter:
Group From Name Filter:  (&(cn=%g)(objectclass=groupOfUniqueNames))
Group Search Scope:  subtree
Group Membership Searching:  unlimited
Max Group Membership Search Level:  0
Ignore Duplicate Membership:  not selected
Static Group Name Attribute: cn
Static Group Object Class:  groupOfUniqueNames
Static Member URL Attribute: uniquemember
Static Group DNs from Member DN Filter:  (&(uniqueMember=%M)
(objectclass=groupOfUniqueNames))
Dynamic Group Name Attribute:
Dynamic Group Object Class:
Dynamic Member URL Attribute:
User Dynamic Group DN Attribute:
Connection Pool Size:  6
Connect Timeout:  60
Connection Retry Limit:  1
Parallel Connect Delay:  0
Results Time Limit: 0
Keep Alive Enabled:  not selected
Follow Referrals: selected
Bind Anonymously On Referrals:  not selected
Propagate Cause For Login Exception: selected
Cache Enabled: selected
Cache Size: 32
Cache TTL:  60
GUID Attribute: entryuuid
```

Example E-2 Sample Provider-specific Values for an Active Directory Provider

```
Host: 10.123.456.789
Port: 389
Principle: CN=StaLdapUser,OU=Users,O=STA,DC=oracle,DC=com
Credential: LDAP (SAM) password
Confirm credential:  LDAP (SAM) password>
SSL Enable: not selected
User Base DN:  OU=Users,O=STA,DC=mycompany,DC=com
All Users Filter:
User From Name Filter: (&(cn=%u)(objectclass=user))
User Search Scope:  subtree
User Name Attribute:  cn
User Object Class:  user
Use Retrieve User Name as Principle:  selected
Group Base DN:  OU=Groups,O=STA,DC=oracle,DC=com
```

```
All Groups Filter:
Group From Name Filter:  (&(cn=%g)(objectclass=group))
Group Search Scope:  subtree
Group Membership Searching:  unlimited
Max Group Membership Search Level:  0
Ignore Duplicate Membership:  not selected
Use Token Groups for Group Membership Lookup:  not selected
Static Group Name Attribute: cn
Static Group Object Class:  group
Static Member URL Attribute: member
Static Group DNs from Member DN Filter:  (&(member=%M)(objectclass=group))
Dynamic Group Name Attribute: >
Dynamic Group Object Class:
Dynamic Member URL Attribute:
User Dynamic Group DN Attribute:
Connection Pool Size:  6
Connect Timeout:  60
Connection Retry Limit:  1
Parallel Connect Delay:  0
Results Time Limit: 0
Keep Alive Enabled:  not selected
Follow Referrals: selected
Bind Anonymously On Referrals:  not selected
Propagate Cause For Login Exception: selected
Cache Enabled: selected
Cache Size: 32
Cache TTL:  60
GUID Attribute: objectguid
```

Set the JAAS Control Flag

The Java Authentication and Authorization Service (JAAS) `Control Flag` attribute assigned to each provider defines whether users must be authenticated by that provider.

The default value for this attribute is "Optional," but for STA, Oracle recommends setting it to "Sufficient" for each provider, including the `DefaultAuthenticator`.

1. Make sure you have locked the active security realm from other users (see Lock the WebLogic Server Active Security Realm).
2. In the Settings for myrealm control bar, select the **Providers** tab.
3. In the Authentication Providers table, select the active link for the provider you want to update.

   IMPORTANT: You must set the control flag for all authentication providers, including the `DefaultAuthenticator`. Do *not* perform this procedure for the `DefaultIdentityAsserter`.

4. In the **Control Flag** menu, select `Sufficient`.

The "Sufficient" setting indicates that if the provider successfully authenticates a user, no additional authentication is required, and if the provider cannot authenticate the user, authentication continues to the next provider in the list. See *Fusion Middleware Securing Oracle WebLogic Server* for descriptions of all options for this attribute.

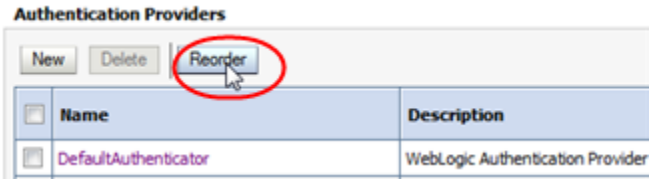
5. Click **Save**.Proceed to Ensure Proper Order of Authentication Providers

Ensure Proper Order of Authentication Providers

When a user attempts to log in to STA, WebLogic Server calls authentication providers in the order they are listed in the Authentication Providers table.

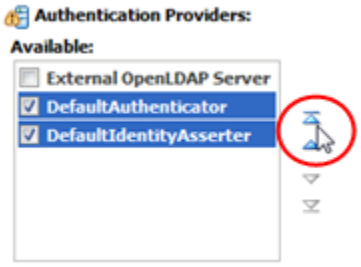
By default, the providers are listed in the order they were added to the active security realm, but you can change their order to better meet the needs of your site. For example, if an external authentication provider includes many STA users, you may want to put that provider at the top of the list so it is called first.

1. Make sure you have locked the active security realm from other users (see Lock the WebLogic Server Active Security Realm).
2. In the Settings for myrealm control bar, select the **Providers** tab.
3. In the Authentication Providers table, click **Reorder**.



4. In the Reorder Authentication Providers table, arrange the providers in the order you want WebLogic Server to access them, from first to last. Select the check box of the providers you want to reorder, then use the arrow buttons to move them up or down in the list.

> **Note:**
>
> The `DefaultAuthenticator` and the `DefaultIdentityAsserter` must be the first two providers in the list.

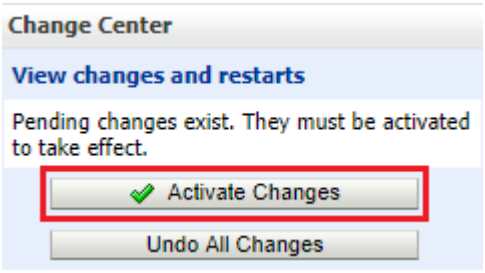


5. When the providers are listed in the order you want, click **OK**.
6. The Authentication Providers table is updated. Proceed to Apply All Configuration Changes.

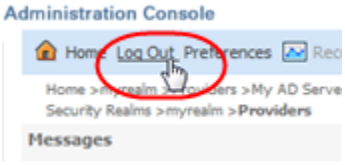
Apply All Configuration Changes

Apply all changes you have made during this editing session. The changes are applied to WebLogic Server and STA.

1. In the Change Center section, click **Activate Changes**.



2. The Messages area indicates that STA must be restarted for the changes to take effect. **Log out** of the WebLogic Administration console.



3. Open a terminal session on the STA server and log in as the Oracle user.
4. Stop and restart STA using the `STA` command. See the *STA Administration Guide* for command usage details.

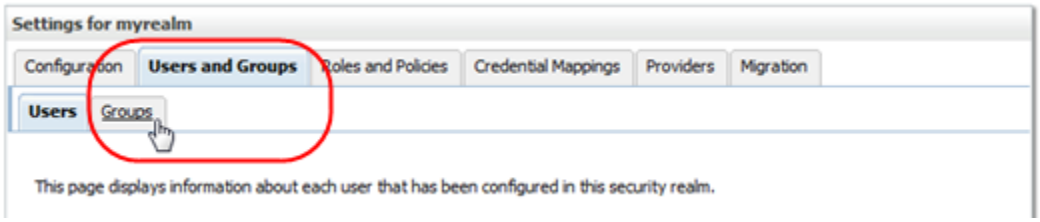
```
$ STA stop all
$ STA start all
```

5. Proceed to Verify Configuration of Authentication Providers.

Verify Configuration of Authentication Providers

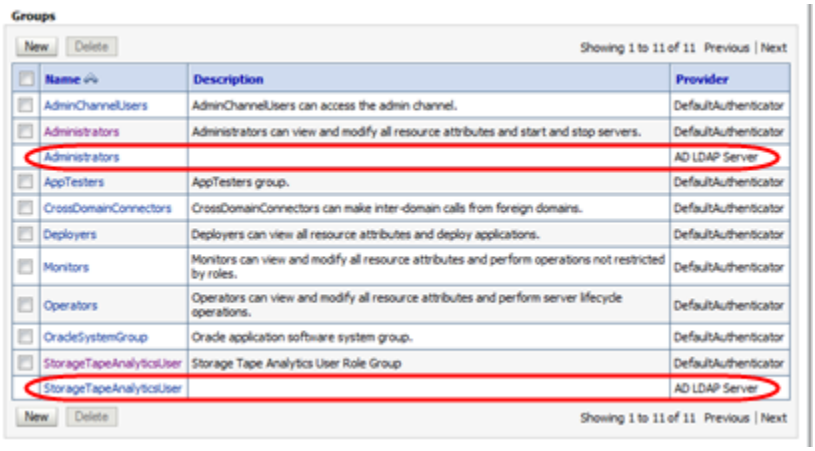
After you have finished configuring one or more external authentication providers for STA, verify that WebLogic Server can access the appropriate users and groups.

1. Log back into WebLogic and make sure you have locked the active security realm from other users (see Lock the WebLogic Server Active Security Realm).
2. In the Settings for myrealm control bar, select the **Users and Groups** tab and then the **Groups** secondary tab.

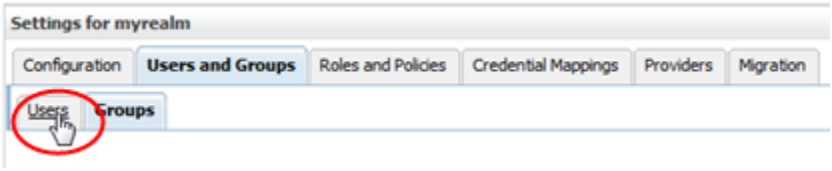


3. Verify that the Groups table includes groups from all configured external authentication providers.

   The following example shows groups from two external providers.

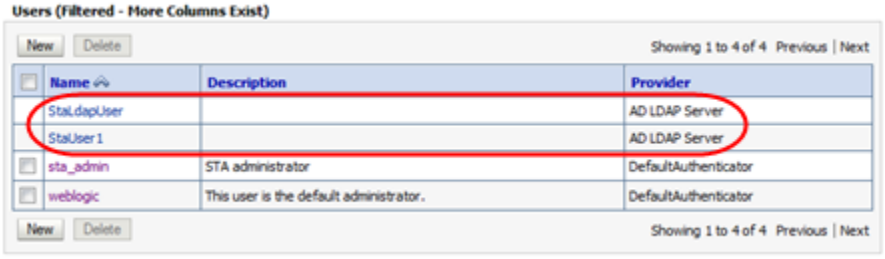


4. In the Settings for myrealm control bar, select the **Users** secondary tab.

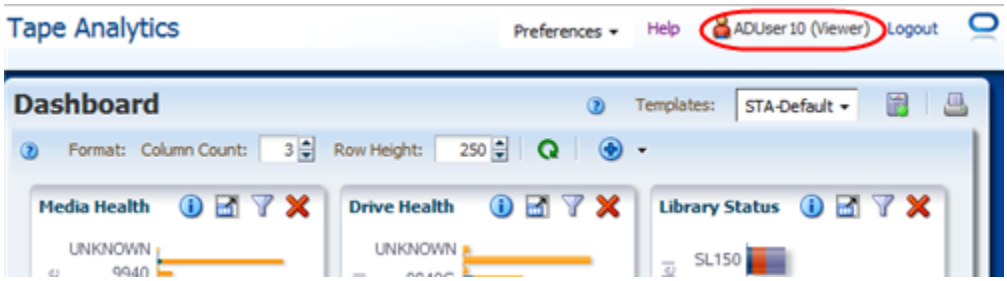


5. Verify that the Users table includes all users assigned to the STA access group (`StorageTapeAnalyticsUser`) on the configured external providers.

   The following example shows users from two external providers.



6. **Log out** of the WebLogic Server Administration console.
7. Go to the STA GUI. Verify that you can use a user account from the external authentication provider to log in to STA and display the Dashboard.



8. STA users from external authentication providers are assigned the STA Viewer role by default. If a user requires a different role (Operator or Administrator), you must modify it manually through the STA user interface. See the *STA User's Guide* for instructions.

Configure IBM RACF Authentication Providers

To configure IBM RACF authentication providers, complete the tasked in the order listed.

- Review IBM RACF Mainframe Minimum Requirements
- Enable Mainframe Support for STA RACF Authorization
- Configure AT-TLS
- Create the RACF Profiles Used by the CGI Routine
- Import the Certificate File and Private Key File (optional)
- Test the CGI Routine
- Set Up RACF/SSP for the WebLogic Console
- Configure SSL Between STA and RACF
- Configure the WebLogic Server
- Install RACF/SSP on the WebLogic Console

Review IBM RACF Mainframe Minimum Requirements

Verify the minimum requirements for IBM RACF.

See the IBM RACF Mainframe Requirements for complete RACF requirements, including required PTFs that must be installed on the MVS system to configure STA authentication with RACF.

> **Note:**
>
> STA supports third-party products that are compatible with IBM RACF—for example, CA's ACF-2 and Top Secret. It is up to the person installing STA, or a security administrator, to issue the commands appropriate for the security product installed.

Enable Mainframe Support for STA RACF Authorization

For STA to use RACF for access authentication, you must setup up an SMC Started Task that runs the HTTP server of the MVS system.

The mainframe side of the RACF service for STA is provided by a CGI routine that is part of the StorageTek Storage Management Component (SMC) for ELS 7.0 and 7.1. This CGI routine is called by the SMC HTTP server and uses RACF profiles defined in the FACILITY class. See the ELS document *Configuring and Managing SMC* for detailed instructions.

The SMC Started Task must match the AT-TLS rule that has been defined. Alternately, allow the AT-TLS definition to use a generic jobname (for example, SMCW). If you are using a value-supplied STC identifier (for example, JOBNAME.JOB), this will cause a CGI routine connection failure.

The port number used for the HTTP server must match the one defined in the WebLogic console, and the host must match the IP name for the host where the SMC task runs.

An existing SMC can be used if it exists on the host where RACF authorization is to be performed. In this case, use the port number of the existing HTTP server when you are performing the WebLogic configuration.

Configure AT-TLS

Configure AT-TLS so the port number defined to the SMC HTTP Server and WebLogic is encrypted to the STA server.

Application Transparent Transport Layer Security (AT-TLS) is an encryption solution for TCP/IP applications that is transparent to the application server and client. Packet encryption and decryption occurs in the z/OS TCPIP address space at the TCP protocol level. AT-TLS requirements for RACF authorization are stated in the IBM RACF Mainframe Requirements.

The following RACF commands list the status of the various RACF objects that you will define in the configuration process:

- `RLIST STARTED PAGENT.* STDATA ALL`
- `RLIST DIGTRING *ALL`
- `RLIST FACILITY IRR.DIGTCERT.LISTRING ALL`
- `RLIST FACILITY IRR.DIGCERT.LST ALL`
- `RLIST FACILITY IRR.DIGCERT.GENCERT ALL`
- `RACDCERT ID(stcuser) LIST`
- `RACDCERT ID(stcuser) LISTRING(keyringname)`
- `RACDCERT CERTAUTH LIST`

Specify Parameter in TCPIP Profile

Specify the following parameter in the TCPIP profile data set to activate AT-TLS.

```
TCPCONFIG TTLS
```

This statement may be placed in the TCP OBEY file.

Configure the Policy Agent (PAGENT)

The Policy Agent address space controls which TCP/IP traffic is encrypted.

1. Enter the PAGENT started task JCL.

   For example:

   ```
   //PAGENT PROC
   //*
   //PAGENT EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
   // PARM='POSIX(ON) ALL31(ON) ENVAR("_CEE_ENVFILE=DD:STDENV")/-d1'
   //*
   //STDENV DD DSN=pagentdataset,DISP=SHR//SYSPRINT DD SYSOUT=*
   //SYSOUT DD SYSOUT=*
   //*
   //CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
   ```

2. Enter the `PAGENT` environment variables. The `pagentdataset` data set contains the `PAGENT` environment variables.

   For example:

   ```
   LIBPATH=/lib:/usr/lib:/usr/lpp/ldapclient/lib:.
   PAGENT_CONFIG_FILE=/etc/pagent.conf
   PAGENT_LOG_FILE=/tmp/pagent.log
   PAGENT_LOG_FILE_CONTROL=3000,2
   _BPXK_SETIBMOPT_TRANSPORT=TCPIP
   TZ=MST7MDT
   ```

   In this example, `/etc/pagent.conf` contains the `PAGENT` configuration parameters. Use your own time zone for the `TZ` parameter.

3. Configure `PAGENT`.

   For example:

   ```
   TTLSRule TBI-TO-ZOS
   {
    LocalAddr localtcpipaddress
    RemoteAddr remotetcpipaddress
    LocalPortRange localportrange
    RemotePortRange remoteportrange
    Jobname HTTPserverJobname
    Direction Inbound
    Priority 255
    TTLSGroupActionRef gAct1~TBI_ICSF
    TTLSEnvironmentActionRef eAct1~TBI_ICSF
    TTLSConnectionActionRef cAct1~TBI_ICSF
   }
   TTLSGroupAction gAct1~TBI_ICSF
   {
    TTLSEnabled On
    Trace 2
   ```

```
}
TTLSEnvironmentAction eAct1~TBI_ICSF
{
 HandshakeRole Server
 EnvironmentUserInstance 0
 TTLSKeyringParmsRef keyR~ZOS
}
TTLSConnectionAction cAct1~TBI_ICSF
{
 HandshakeRole ServerWithClientAuth
 TTLSCipherParmsRef cipher1~AT-TLS__Gold
 TTLSConnectionAdvancedParmsRef cAdv1~TBI_ICSF
 CtraceClearText Off
 Trace 2
}
TTLSConnectionAdvancedParms cAdv1~TBI_ICSF
{
 ApplicationControlled Off
 HandshakeTimeout 10
 ResetCipherTimer 0
 CertificateLabel certificatelabel
 SecondaryMap Off
}
TTLSKeyringParms keyR~ZOS
{
 Keyring keyringname
}
TTLSCipherParms cipher1~AT-TLS__Gold
{
 V3CipherSuites TLS_RSA_WITH_3DES_EDE_CBC_SHA
 V3CipherSuites TLS_RSA_WITH_AES_128_CBC_SHA
}
```

where:

- `localtcpipaddress`: Local TCP/IP address for the HTTP server
- `remotetcpipaddress`: Remote TCP/IP address for the STA client. This can be ALL for all TCP/IP addresses
- `localportrange`: Local port of HTTP server (specified in the HTTP or SMC startup)
- `remoteportrange`: Remote port range (1024-65535 for all ephemeral ports)
- `HTTPserverJobname`: Jobname of the HTTP Server
- `certificatelabel`: Label from the certificate definition
- `keyringname`: Name from the RACF keyring definition

Activate RACF Classes

Either the RACF panels or the CLI can be used.

The RACF classes include:

- `DIGTCERT`
- `DIGTNMAP`
- `DIGTRING`
- `SERVAUTH` class must be RACLISTed to prevent `PORTMAP` and `RXSERV` from abending.

```
SETROPTS RACLIST(SERVAUTH)
RDEFINE SERVAUTH **UACC(ALTER) OWNER (RACFADM)
RDEFINE STARTED PAGENT*.* OWNER(RACFADM) STDATA(USER(TCPIP) GROUP(STCGROUP)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE) OWNER(RACFADM)
RDEFINE FACLITY IRR.DIGTCERT.LIST UACC(NONE) OWNER(RACFADM)
RDEFINE FACILITY IRR.DIGTCERT.GENCERT UACC(NONE) OWNER (RACFADM)
```

Define RACF Keyrings and Certificates

Enter the following RACF commands to create Keyrings and certificates:

RACDCERT ID(*stcuser*) ADDRING(*keyringname*)

where:

- `stcuser`: RACF user id associated with the TCPIP address space
- `keyringname`: Name of the keyring, must match the Keyring specified in the PAGENT configuration

For the CA certificate for the STA system:

```
RACDCERT ID(stcuser) GENCERT CERTAUTH SUBJECTSDN(CN('serverdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('calabel') TRUST
SIZE(1024) KEYUSAGE(HANDSHAKE,DATAENCRYPT,CERTSIGN)
```

where:

- `stcuser`: RACF user id associated with the TCPIP address space
- `serverdomainname`: Domain name of the z/OS server
- `companyname`: Organization name
- `unitname`: Organizational unit name
- `country`: Country
- `calabel`: Label for certificate authority (for example, CATBISERVER)

For the SERVER certificate:

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('serverdomainname') O('companyname')
OU('unitname') C('country')) WITHLABEL('serverlabel') TRUST SIZE(1024)
SIGNWITH(CERTAUTH LABEL('calabel'))
```

where:

- `stcuser`: RACF user id associated with the TCPIP address space
- `serverdomainname`: Domain name of the z/OS server
- `companyname`: Organization name
- `unitname`: Organizational unit name
- `country`: Country
- `serverlabel`: Label for the server certificate (for example, TBISERVER)
- `calabel`: Label for certificate authority, specified in the CA certificate definition

For the CLIENT certificate:

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('clientdomainname') O('companyname')
OU('unitname') C('country')) WITHLABEL('clientlabel') TRUST SIZE(1024)
SIGNWITH(CERTAUTH LABEL('calabel'))
```

where:

- `stcuser`: RACF user id associated with the TCPIP address space
- `clientdomainname`: Domain name of the STA client
- `companyname`: Organization name
- `unitname`: Organizational unit name
- `country`: Country
- `clientlabel`: Label for the server certificate –TBICLIENT
- `calabel`: Label for certificate authority, specified in the CA certificate definition.

Connect the CA, SERVER, and CLIENT certificates to the keyring specified in the PAGENT configuration

Connect the CA, SERVER, and CLIENT certificates to the keyring :

```
RACDCERT ID(stcuser) CONNECT(CERTAUTH LABEL('calabel') RING('keyringname')
USAGE(CERTAUTH))
```

where:

- `stcuser`: RACF user id associated with the TCPIP address space
- `calabel`: Label for certificate authority, specified in the CA certificate definition
- `keyringname`: Name of the keyring, must match the Keyring specified in the PAGENT configuration

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('serverlabel') RING('keyingname')
DEFAULT USEAGE(PERSONAL)
```

where:

- `stcuser`: RACF user id associated with the TCPIP address space
- `serverlabel`: Label for the server certificate
- `keyringname`: Name of keyring, must match the Keyring specified in the PAGENT configuration

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('clientlabel') RING('keyingname')
USEAGE(PERSONAL)
```

where:

- `stcuser`: RACF user id associated with the TCPIP address space
- `clientlabel`: Label for the client certificate
- `keyringname`: Name of keyring, must match the Keyring specified in the PAGENT configuration

Export the CA and client certificates to be transmitted to STA

```
RACDCERT EXPORT (LABEL('calabel')) CERTAUTH DSN('datasetname') FORMAT(CERTB64)
```

where:

- `calabel`: Label for certificate authority, specified in the CA certificate definition
- `datasetname`: Data set to receive the exported certificate

```
RACDCERT EXPORT (LABEL('clientlabel')) ID(stcuser) DSN('datasetname')
FORMAT(PKCS12DER) PASSWORD(' password ')
```

where:

- `clientlabel`: Label for the client certificate
- `stcuser`: RACF user id associated with the TCPIP address space
- `datasetname`: Data set to receive the exported certificate
- `password`: Password for data encryption. Needed when the certificate is received on STA. The password must be eight characters or more.

The export data sets are now transmitted to STA, and FTP can be used. The CA certificate is transmitted with an EBCDIC to ASCII conversion. The CLIENT certificate is transmitted as a BINARY file and contains both the client certificate and its private key.

Create the RACF Profiles Used by the CGI Routine

The profiles are defined in the FACILITY class. The first of the profiles is called `SMC.ACCESS.STA` and determines whether a user has access to the STA application.

A user who requires access to STA must have READ access to this profile. The other profiles are all shown as `SMC.ROLE.nnn` and are used to determine which roles the user has once logged on.

> **Note:**
>
> The only role defined to STA is `StorageTapeAnalyticsUser`. To obtain this role, you must request your user ID to be added to the `SMC.ROLE.STORAGETAPEANALYTICSUSER` profile with READ access.

Import the Certificate File and Private Key File (optional)

Verify that public and private keys have been generated successfully and that user IDs and passwords with the appropriate permissions have been defined correctly.

The test can be done using any browser, but Firefox is used here as an example.

1. In the Firefox **Tools** menu, select **Options**.
2. Select the **Advanced** tab, and then select the **Encryption** tab.
3. Click **View Certificates**.
4. In the Certificate Manager dialog box, select the **Authorities** tab, and then select the certificate file to import.
5. Click **Import**.

6. Select the **Your Certificates** tab, and then enter the private key file to import.
7. Click **Import**.
8. Click **OK** to save and exit the dialog box.

Test the CGI Routine

Test the CGI routine from a browser.

- Open a browser window, and enter the following URL, where `host`, `port`, `userid`, and `password` are set to appropriate values.

  https://*host*:*port*/**smcgsaf?type=authentication&userid=***userid*&password=*password*&roles=StorageTapeAnalyticsUser**

  The resulting output indicates whether the user is authorized to access STA and the `StorageTapeAnalyticsUser` role.

> **Note:**
>
> The STA RACF authorization facility does not support changing the password of mainframe user IDs. If a user ID password expires, STA indicates this, and the password must be reset through normal mainframe channels before attempting to log in to STA again.

Set Up RACF/SSP for the WebLogic Console

The RACF Security Service Provider (or RACF SSP) must be installed as a WebLogic plug-in. If the RACF SSP has been installed, the STA installer should put the RACF SSP in the appropriate location within WebLogic.

Place the RACF SSP in the proper location, if it has not been already.

- Place the RACF security jar file into the following directory:

  /*Oracle_storage_home*/Middleware/wlserver_10.3/server/lib/mbeantypes/staRACF.jar

  where `Oracle_storage_home` is the Oracle storage home location specified during STA installation.

Configure SSL Between STA and RACF

Install the MVS security certificate on the STA server and import it into the systemwide Java keystore.

1. Verify that the required PTFs have been installed on the MVS system. These PTFs allow for authentication with RACF or other third-party security software when you log in to the STA application. See Review IBM RACF Mainframe Minimum Requirements for details.
2. Obtain the following files:
   - MVS server certificate, in ASCII format
   - STA client private key, in binary PKCS12 format; the MVS system administrator should give you the password to this file.

3. Transfer the files to the STA server, and place them in the certificates directory. The directory location is as follows:

   /Oracle_storage_home/Middleware/user_projects/domains/TBI/cert

   where Oracle_storage_home is the Oracle storage home location specified during STA installation.

4. Convert the certificate from Distinguished Encoding Rules (DER) format to Privacy Enhanced Mail (PEM) format. For example:

   ```
   $ openssl pkcs12 -clcerts -in PKCS12DR.xxxxxx -out mycert.pem
   ```

   Where:

   - pkcs12 indicates PKCS#12 data management.
   - -clcerts indicates you want to output client certifications only.
   - -in specifies the input file.
   - -out specifies the output file.

   You will be asked to enter the import password (given to you with the certificate), a new PEM password, and password verification.

5. Change to the JRE binary directory. The directory location is as follows:

   /Oracle_storage_home/StorageTek_Tape_Analytics/jdk/jre/bin

   where Oracle_storage_home is the Oracle storage home location specified during STA installation.

   For example:

   ```
   $ cd /Oracle/StorageTek_Tape-Analytics/jdk/jre/bin
   ```

6. Use the Java keytool utility to import the certificate file into the systemwide Java keystore. The keystore is located in the following file:

   /Oracle_storage_home/StorageTek_Tape_Analytics/jdk1.6.0_xx/jre/lib/security/cacerts

   For example:

   ```
   $ ./keytool -importcert -alias tbiServer -file mycert.pem -keystore /Oracle/
   StorageTek_Tape_Analytics/jdk1.6.0_75/jre/lib/security/cacerts -storetype jks
   ```

   Where:

   - -importcert indicates you want to import a certificate.
   - -alias indicates the name you want to assign to the entry in the keystore.
   - -file indicates the name of the certificate file you want to import.
   - -keystore indicates the location of the systemwide Java keystore.
   - -storetype indicates the type of keystore.

Configure the WebLogic Server

Configure the WebLogic server for RACF authentication.

Use the procedure in Reconfigure WebLogic to use a Different Security Certificate.

Install RACF/SSP on the WebLogic Console

Install the RACF/SSP on the WebLogic console to complete the authentication setup.

1. Go to the WebLogic console login screen using the HTTP (STA 2.1.x default is 7019) or HTTPS (STA 2.1.x default is 7020) port number you selected during STA installation.

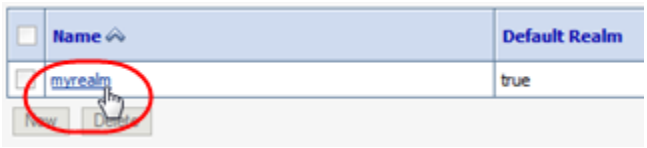
   `https://`*`yourHostName`*`:`*`PortNumber`*`/console/`

   For example:

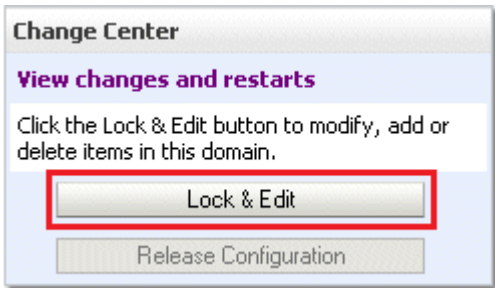
   `https://sta_server:7020/console/`

2. Log in using the WebLogic administration console username and password you defined during STA installation.
3. In the Domain Structure section, select **Security Realms**.

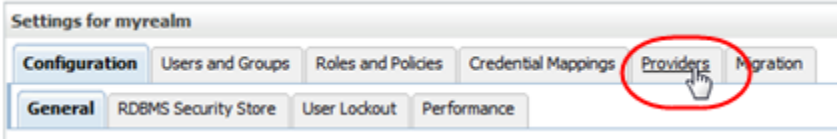
4. In the Realms section, select the **myrealm** active link (select the name itself, not the check box).



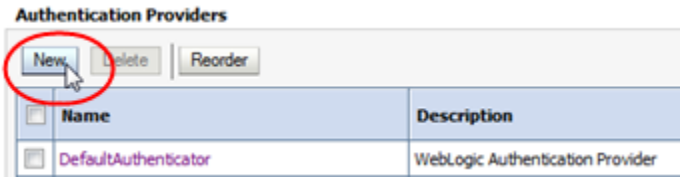
5. In the Change Center section, click **Lock & Edit**.



6. Select the **Providers** tab.



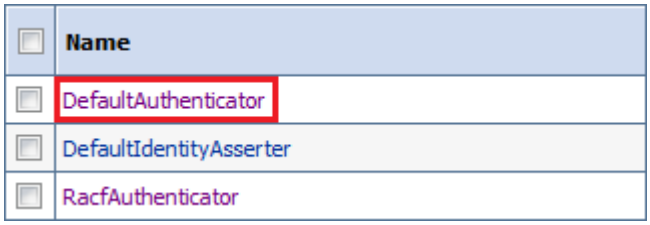
7. In the Authentication Providers section, click **New**.



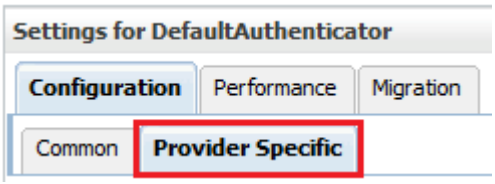
8. Enter the name of the authentication provider you want to add (for example, `STA RacfAuthenticator`), and select `RacfAuthenticator` in the **Type** menu. Click **OK**.

> **Note:**
>
> The RACF jar file should be listed in the **Type** menu. If it is not, stop and restart STA using the `STA` command. See the *STA Administration Guide* for command usage details.

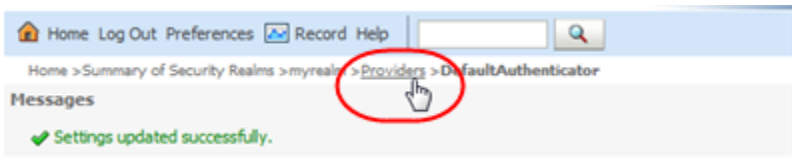
9. Verify the RACF provider is included in the Authentication Providers table. The `DefaultAuthenticator` and `DefaultIdentityAsserter` must always be the first two providers in this list.
10. Select the **DefaultAuthenticator** active link (select the name itself, not the check box).



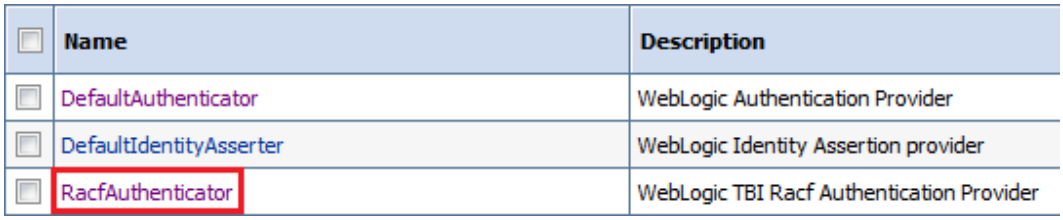
11. In the **Control Flag** menu, select Sufficient, and then click **Save**.
12. Click the **Provider Specific** tab, and then click **Save**.



13. Click the **Providers** locator link to return to the Authentication Providers screen.

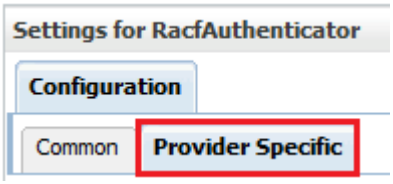


14. In the Authentication Providers table, select the RACF authenticator name you created in Step 8 (select the name itself, not the check box).

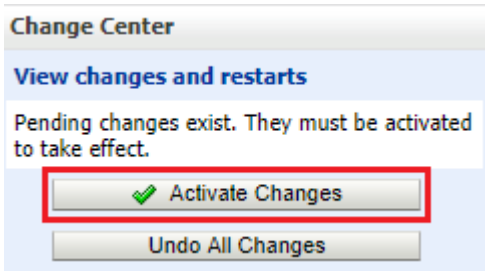


15. In the **Control Flag** menu, select `Sufficient`, and then click **Save**.

16. Click the **Provider Specific** tab.



17. Enter the Host name (for example, `mvshost.yourcompany.com`) and Port number (for example, `8700`) where the MVS system is running, and then click **Save**.
18. In the Change Center section, click **Activate Changes**.



19. Log out of the WebLogic Administration console.
20. Stop and restart STA using the `STA` command. See the *STA Administration Guide* for command usage details.

```
$ STA stop all
$ STA start all
```

F

Troubleshoot Issues

Many issues you may encounter have a workaround or simple resolution.

GUI Issues

- ISSUE: Cannot Access the STA GUI
- ISSUE: GUI Elements Do Not Render Correctly

Data Issues

- ISSUE: Exchanges Not Showing Up in STA
- ISSUE: T10000D Drives Are Not Showing Quality Index After Media Validation

Connection Issues

- ISSUE: Database Communication Link Failure (IMPORTANT)
- ISSUE: OSCI Library Connection Test Fails
- ISSUE: SNMP Library Connection Test Fails
- ISSUE: SNMP Trap Status Not Updating After Connection Test
- ISSUE: Cannot Connect to SDP

Server Process and Installation Issues

- ISSUE: STA Fails to Restart Properly After Reboot
- ISSUE: Weblogic Server Processes Not Starting
- ISSUE: Authentication Prompts During STA start Command
- ISSUE: Backup Service or Resource Monitor Fails
- ISSUE: MySQL Installation Fails
- ISSUE: STA Does Not Completely Deinstall

ISSUE: Cannot Access the STA GUI

If you cannot access the STA GUI, first verify STA is running. Then, verify the firewall settings and iptables.

Resolution

1. Verify STA is running by using the command:

   ```
   # STA status all
   ```

2. Verify you are using the correct URL:

   ```
   http://<server name or IP address>:7021/STA
   ```

   OR

   ```
   https://<server name or IP address>:7022/STA
   ```

Ports 7021 and 7022 are the default installer port numbers. If you customized or changed the port numbers, use the corresponding custom port numbers instead.

3. If STA is running and you still cannot access the GUI, verify the following firewall settings:
   - Firewall is running
   - Check hosts.allow and hosts.deny files if using those OS services
   - REJECT rules are not interfering with the GUI ports (such as 162 and 7029)

   To verify, open a terminal session and login as the root user. Issue the following:

   ```
   # systemctl status iptables
   # iptables -L
   ```

4. If needed, use the iptables command to remove or modify the firewall rules to allow access to the STA GUI. For example:

   ```
   # iptables -D INPUT 5
   ```

   > **WARNING:**
   >
   > Removing or modifying firewall rules can create security risks and must be done by qualified security administrator.

5. If the GUI was inaccessible after a server reboot occurred, verify the iptables:
   a. Verify iptables rules were been saved correctly using the service iptables save command.

      ```
      # service iptables save
      ```

   b. Verify the iptables server is enabled. For example

      ```
      # systemctl status iptables
      # systemctl start iptables
      # systemctl enable iptables
      ```

ISSUE: GUI Elements Do Not Render Correctly

When using a browser tab that you previously used for a now expired STA session, various elements may not work as expected. Logging out or terminating the browser session can correct this issue.

An improperly closed-out and expired STA session may cause the UI infrastructure to apply stale information which it cannot render. This behavior is not browser-specific. It can occur on various browser platforms.

Symptoms

- Navigation bar may not contain all normal entries
- Pages may render, but without all expected elements
- User customizations (like custom templates and defaults) may not appear
- Dialog boxes may fail to launch or may not respond to input
- Interface may fail to respond to input or appear frozen

The staUi log will contain `RESTORE_VIEW` errors. These errors are usually followed by another more specific indicator like “null windowId”, “page has expired”, “Could not find saved view state”, and so on.

Workaround

This error is non-destructive. There are several options to work around it:

- Always click **Logout** to terminate your STA sessions. If you do so, the error will not occur.
- If you forgot to logout of the previous session, click **Logout** on the current session. This will clean out the UI state. Then, you can log back into STA.
- Terminate the browser tab and open a new tab to log into STA.

ISSUE: Exchanges Not Showing Up in STA

If exchanges are not showing up within STA, the SNMP traps from the library may not be reaching STA. You should verify the SNMP configuration and verify the iptables.

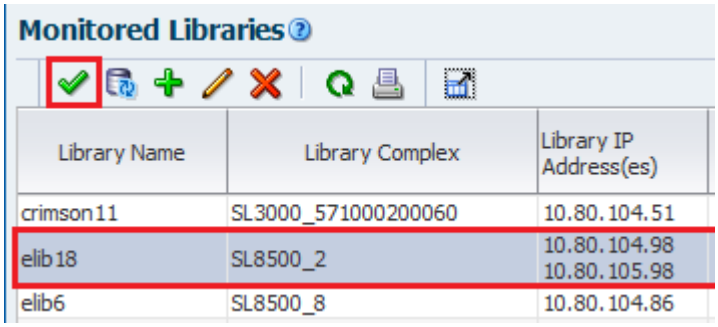
Verify STA is Running

1. Open a terminal session on the STA server, and login in as the Oracle user.
2. Verify STA is running by using the command:

```
$ STA status all
```

Test the SNMP Connection

1. Sign in to the STA GUI. In the left navigation, expand **Setup & Administration**, then click **Library Connections**.
2. Within the Monitored Libraries table, select the library in question and click **Test Connection** ✔.



If the MIB Walk or Trap Channel tests **FAIL**, see the following sections in the Installation and Configuration Guide "Configure SNMP" chapter:

- "Troubleshoot a Failed MIB Walk Channel Test"
- "Troubleshoot a Failed Trap Channel Test"
- If these do not correct the issue, proceed to Verify Network Configuration.

If the tests **PASS**, proceed to Verify iptables Configuration.

Verify Network Configuration

1. If STA is running but the connection test fails, verify the following:
   - Firewall is running (also known as iptables)
   - hosts.allow and hosts.deny files (if using those services). You may need to add the library IP address to hosts.allow.
   - REJECT rules do not interfere with the GUI ports (for example 162 and 7029)
   - Port forwarding from 162 to 7029 (port 7029 may be different if you have customized it)
   - Network router configuration between the STA server and library. Some routers may drop UDP or SNMP packets.

   To verify STA server settings, login as the root user and use the following commands:

```
# systemctl status iptables
# more /etc/hosts.allow
# iptables -L
# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target    prot opt source    destination
REDIRECT  udp  --  anywhere  anywhere    udp  dpt:snmptrap redir ports 7027
```

2. If needed, use the iptables command to add port forwarding or remove and modify the rules to all SNMP traps.

Verify iptables Configuration

A server reboot can cause an issue with the iptable configuration. If the issue occurred following a reboot, verify the iptables are correct.

1. Use service iptables save command to verify the iptables rules are saved correctly.

```
# service iptables save
```

2. Verify the iptables server is enabled. For example::

```
# systemctl status iptables
# systemctl start iptables
# systemctl enable iptables
```

ISSUE: T10000D Drives Are Not Showing Quality Index After Media Validation

The T10000D drives must have both *Level 3 Media Validation* and *Level 3 RQI Margin Report* enabled within VOP to report Quality Index values.

Verify the VOP Settings

1. Within VOP, under the **Retrieve** menu, select **View Drive Data**.
2. Select the **Maintenance** tab.
3. Check that both *Level 3 Media Validation* and *Level 3 RQI Margin Report* are enabled.

4. If not, follow the steps below to enable both of these settings.

Enable the Settings

1. Set the drive offline. Within the **Drive Operations** menu, select **Set Offline**.
2. Within the **Configuration** menu, select **Drive Data**.
3. Select the **Maintenance** tab.
4. Enable *Level 3 Media Validation* and *Level 3 RQI Margin Report*.
5. Click **Commit**. The drive will IPL.
6. Retry the media validation.

ISSUE: Database Communication Link Failure (IMPORTANT)

Database communication link failures can occur if there are duplicate iptable rules.

The following exceptions in the Weblogic logs indicate a database communication issue: `com.mysql.jdbc.exceptions.jdbc4.CommunicationsException: Communications link failure`.

To correct the issue:

1. Have the network administrator review the iptable rules.
2. Remove duplicate or overlapping iptable rules.
3. Stop and restart STA:

```
$ STA stop all
$ STA start all
```

ISSUE: OSCI Library Connection Test Fails

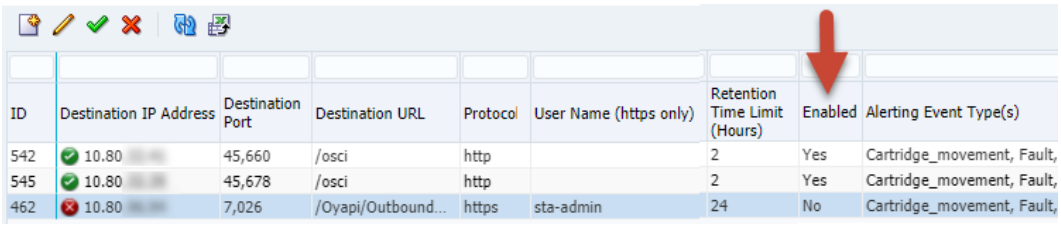
The OSCI connection test may fail if the destination is not enabled within the SL4000 user interface.

Access the SL4000 GUI Notifications Page

1. Log into the SL4000 GUI.
2. Click **Notifications** in the left navigation area.
3. Click the **SCI** tab.

Verify the Destination is Enabled

1. Verify the **Enabled** column for the STA destination says **Yes**.



ID	Destination IP Address	Destination Port	Destination URL	Protocol	User Name (https only)	Retention Time Limit (Hours)	Enabled	Alerting Event Type(s)
542	10.80	45,660	/osci	http		2	Yes	Cartridge_movement, Fault,
545	10.80	45,678	/osci	http		2	Yes	Cartridge_movement, Fault,
462	10.80	7,026	/Oyapi/Outbound...	https	sta-admin	24	No	Cartridge_movement, Fault,

2. If not, select the STA destination in the table and then click **Edit** .
3. Check the **Enabled** box, and then click **Ok**.

ISSUE: SNMP Library Connection Test Fails

The SNMP library connection test may fail for multiple reasons such as iptables configuration.

If the connection test failure is occurring with an SL150 library, be sure to verify firewall rules.

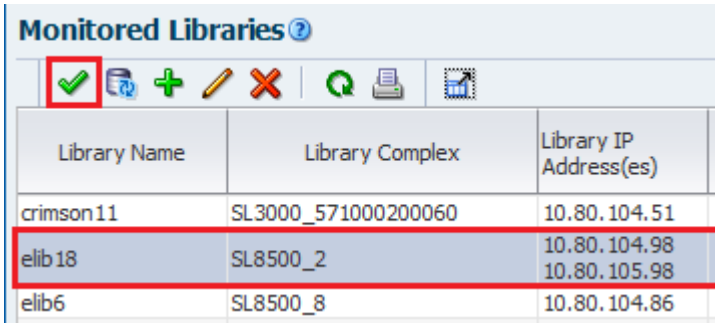
Refer to ISSUE: Exchanges Not Showing Up in STA for details on how to troubleshoot this issue.

ISSUE: SNMP Trap Status Not Updating After Connection Test

The SNMP configuration screen may not update immediately after a connection test, even after a refresh, but you can run the connection test again and use the values provided by the Test Connection dialog to confirm the status.

Workaround

1. Sign in to the STA GUI. In the left navigation, expand **Setup & Administration**, then click **Library Connections**.
2. Within the Monitored Libraries table, select the library in question and click **Test Connection** .



3. Use the values reported by the test to verify the status.

   Such as:

   - MIB Walk Channel :: Good (SNMP V3)
   - Trap Channel :: Good (SNMP V3)
   - Media Validation Support :: Good

ISSUE: Cannot Connect to SDP

STA may not be able to connect to SDP due to a hostname mismatch. Adding an entry to the /etc/hosts file on the STA server can resolve this issue.

Symptom

SDP status within the STA GUI indicates "Unable to contact or connect to SDP host".

This can occur if the SDP server hostname defined on the public name servers does not match the hostname sent within the ASR packets. For example, the SDP server sends an ASR packet with its name as "sdp2host" but the name defined on the public name servers is "sdp2server.mycompany.com".

Resolution

Define the SDP host in the /etc/hosts file on the STA server. Add an entry with the IP address of the SDP server and the hostname that the SDP server provides in the ASR packets. For example, "10.20.30.40 sdp2host".

ISSUE: STA Fails to Restart Properly After Reboot

Sometimes STA fails to restart properly after the system reboots on Linux 7 systems using systemd services. Stopping and starting STA should resolve this issue.

1. Open a terminal session on the STA server.
2. Stop and restart STA.

```
$ STA stop all
$ STA start all
```

ISSUE: Weblogic Server Processes Not Starting

After a server reboot or non-graceful shutdown of STA, one of the Weblogic server processes like (staAdapter, staEngine, staUi, AdminServer) may not start. This can be caused by a Weblogic lock file (.lck) that was not properly removed during shutdown.

Resolution

1. Open a terminal session on the STA server and login as the Oracle user.
2. Examine the Weblogic log files for the services that have not started. Look for errors or the presence of a .lck file.

   The log files are located in:

   ```
   TBI/servers/AdminServer/logs/weblogic.log
   TBI/servers/staAdapter/logs/weblogic_staAdapter.log
   TBI/servers/staUi/logs/weblogic_staUi.log
   TBI/servers/staEngine/logs/weblogic_staEngine.log
   ```

3. Use the `rm -f` command to remove the lock file for the STA server process that has not started.
4. Restart STA using the command:

```
$ STA start all
```

ISSUE: Authentication Prompts During STA start Command

When using Linux 7 or 8, you may see an authentication message after using the STA start command. The message should time out and the STA service should start. Or the server administrator can add polkit rules to remove the authentication requests.

Symptom

While using the STA start command the following authentication messages appear:

```
Starting staweblogic Service.==== AUTHENTICATING FOR
org.freedesktop.systemd1.manage-units ===
Authentication is required to manage system services or units.
Authenticating as: root
```

Resolution

The OS polkit service running on the server generates this message. Depending on the server configuration this authentication prompt (password prompt) will time out and STA services will start normally.

If the authenticate does interfere with STA service starting, then contact your server administrator. The administrator can add polkit rules to remove the authentication requests in the following location:

```
/usr/share/polkit-1/rules.d/org.freedesktop.systemd1.manage-units.rules
```

> **WARNING:**
>
> Modifying polkit rules can create security risks and must be done by qualified security administrator.

ISSUE: Backup Service or Resource Monitor Fails

The Backup Service or Resource Monitor may fail if the Oracle user does not have write access to /etc/.java or `staservd` does not have write access to /etc/.java/.systemPrefs.

Symptom

The service fails with the following:

```
Error: java.util.prefs.BackingStoreException: Couldn't get file lock.
```

Resolution

1. Open a terminal session on the STA server and login as the root user.
2. Provide write access to the `/etc/.java` and `/etc/.java/.systemPrefs` directories. For example:

```
# chmod 777 /etc/.java
# chmod 777 /etc/.java/.systemPrefs
```

3. Switch to the Oracle user.
4. Stop the services daemon:

```
$ STA stop staservd
$ STA status staservd
```

You should see: `staservd service is shutdown`

5. Start the services daemon:

```
$ STA start staservd
```

ISSUE: MySQL Installation Fails

If the installation fails to install MySQL, you may need to restart the server and retry the installation.

Symptom

You may encounter 'ERROR 2002 (HY000): Can't connect to local MySQL server through socket'.

Workaround

Keep retrying the install until the installation does not hit the timing window which is causing this issue.

1. Reboot the server, then retry the installation.
2. Retry the installation using the other installer type (meaning try the silent installer if you previously used the GUI installer or vice versa).

ISSUE: STA Does Not Completely Deinstall

If the deinstallation of STA fails or fails to uninstall everything, you may need to manually remove components of STA.

The following steps assume that the Storage Home is `/Oracle` and the Oracle Inventory Home is `/Oracle`. If these values differ for your system, adjust the steps below.

Some of the steps may fail because the component may already be uninstalled.

1. Start a terminal session as the 'root' super user.
2. Stop the WebLogic processes:

```
# STA stop all
```

3. Stop MySQL:

```
# service mysql stop
```

4. Stop any remaining oracle processes (this assumes the oracle user was used to install STA, otherwise adjust appropriately).

```
# ps -eaf | grep oracle
# kill -9 <pids>
```

Repeat until all oracle processes have been killed.

5. Remove the following directories:

```
# rm -rf /Oracle/Middleware
# rm -rf /Oracle/StorageTek_Tape_Analytics/
```

6. Identify any installed MySQL packages:

```
# yum list MySQL*
```

7. Remove the MySQL packages:

```
# yum remove MySQL*
```

8. Remove the following directories:

```
# rm -rf /usr/bin/STA
# rm -rf /Oracle/oraInventory
# rm -f /etc/oraInst.loc
```