

StorageTek Tape Analytics
Installation and Configuration Guide
Version 2.2.0
E68628-01

February 2016

Primary Author: Nancy Stevens

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	xi
Audience	xi
Documentation Accessibility	xi
Related Documents	xi
Conventions	xii
What's New	xiii
STA 2.2.0 February 2016	xiii
1 Pre-installation Planning	
STA Deployment Process Overview	1-1
Best Practices for STA Deployment	1-2
Preparation.....	1-2
Linux Installation	1-2
STA Installation	1-3
Library Configuration for STA.....	1-3
SNMP Connections With the Libraries.....	1-4
Data Collections.....	1-4
STA Services Configuration.....	1-5
STA Database Tuning.....	1-5
Prepare Service Requests for the Libraries and Drives	1-5
2 Installing Linux	
Linux Installation Process	2-1
Preparation Tasks	2-2
Review Related Documentation	2-2
Review STA File System Layout.....	2-2
Download the Linux Installer Media Pack.....	2-3
Installation Tasks	2-4
Gather Required Information.....	2-4
Install Linux	2-4
Run the Linux Setup Agent	2-6
Post-Installation Tasks	2-7
Ensure the Correct root User Path.....	2-8
Disable the Linux Firewall.....	2-8

Disable SELinux	2-9
Remove SELinux Permissions.....	2-9
Set Up the Network Proxy.....	2-10
Ensure Proper Setup of yum (optional).....	2-10
Install Required Linux Packages.....	2-11
Ensure Proper Setup of SSH.....	2-12
Ensure Proper DNS Settings.....	2-12
Disable Name Services	2-12
Ensure Local Browser Functionality (optional).....	2-13

3 Installing STA

Users, Groups, and Locations Used by the STA Installer	3-1
Username and Password Requirements	3-3
Accounts and Ports Configured During STA Installation	3-3
User Accounts for Managing STA.....	3-3
Ports Used by STA	3-4
STA Installation and Deinstallation Logs	3-6
Log File Locations	3-6
STA Installer Modes	3-7
STA Installation Tasks	3-7
Identify or Create Information Required for the Installation	3-7
Verify Installation Prerequisites.....	3-9
Download STA	3-11
Install STA	3-16
Verify Successful Installation	3-17
Relocate the STA Logs Directory (optional).....	3-18
Register the Oracle Central Inventory Location	3-19
Display the Oracle Central Inventory Location.....	3-19

4 Configuring Library Features for STA

Library Features Affecting STA Data	4-1
ADI Interface for LTO Drives.....	4-1
Dual TCP/IP and Redundant Electronics (SL3000 and SL8500 only).....	4-2
Library Complex ID (SL8500 only).....	4-3
Drive Clean Warning (SL3000 and SL8500 only)	4-4
Volume Label Format (SL500 and SL150 only).....	4-4
SCSI FastLoad Option (SL500 only)	4-5
Duplicate Volume Serial Numbers	4-5
Library User Interfaces	4-5
Library CLI Usage Tips	4-5
Library Configuration Script (optional).....	4-6
Library Feature Configuration Tasks	4-6
Log In to the Library.....	4-7
Verify the Library Firmware Version.....	4-7
Verify the Drive Controller Card Version (SL3000 and SL8500 only).....	4-8
Enable ADI on the Library (all libraries except SL150)	4-9
Ensure the Correct Library Complex ID (SL8500 only).....	4-9

Set the Drive Clean Warning (optional, SL3000 and SL8500 only).....	4-10
Set the SL500 Volume Label Format (SL500 only)	4-10
Set the SL150 Volume Label Format and Drive Element Addressing Mode (SL150 only) ..	4-11

5 Configuring SNMP on the Libraries

Understanding Library SNMP Configuration for STA	5-1
Configuring the SNMP v3 Protocol on the Libraries	5-1
Library SNMP Configuration Tasks	5-3
Retrieve the Library IP Address.....	5-4
Enable SNMP on the Library.....	5-5
Ensure an SNMP v2c User	5-6
Create an SNMP v3 User.....	5-7
Retrieve the Library SNMP Engine ID (all libraries except SL150)	5-8
Create the STA SNMP v3 Trap Recipient.....	5-8

6 Configuring Library Connections in STA

STA Configuration Tasks	6-1
Log In to STA	6-1
Verify SNMP Communication With a Library	6-2
Configure SNMP Client Settings for STA.....	6-4
Configure the SNMP Connection to a Library	6-5
Test a Library SNMP Connection	6-7
Perform a Manual Data Collection	6-9

7 Configuring STA Services

STA Services Overview	7-1
STA Services Configuration Tasks	7-1
Update the System Path (optional).....	7-2
Restart the STA Services Daemon (optional)	7-2
Verify Library Connectivity.....	7-2
Review the STA Database Backup Utility Preferences	7-2
Configure the Remote Database Backup Server.....	7-3
Configure the STA Database Backup Service	7-4
Review the STA Resource Monitor Utility Preferences.....	7-5
Configure the STA Resource Monitor	7-7

8 Upgrading to STA 2.2.x

Upgrade Paths	8-1
Upgrade Process Overview	8-2
Preparing for the Upgrade.....	8-2
Understanding Automatic and Post-installation Upgrades	8-2
Post-installation Upgrades: Choosing Whether to Use One Server or Two.....	8-3
Environment Changes	8-5
Linux Version.....	8-5
Default WebLogic Port Numbers	8-5

Username and Password Requirements	8-6
Required Ports for STA	8-6
Preparation Tasks for All Upgrades	8-7
Verify Your Site is Ready for the Upgrade	8-7
Save Existing Logs (optional)	8-8
Record Current STA User and Configuration Settings (optional)	8-9
Rename Custom Templates With STA- Prefix (optional)	8-13
Record Current Custom Template Settings (optional)	8-14
Record Executive Report Policy Settings (optional)	8-14
Post-installation Upgrade Tasks	8-15
Task 1: Dump the Old STA Database	8-15
Task 2: Transfer the Old Database Dump	8-16
Task 3a: Install the New Linux Version—Upgrades From STA 1.0.x	8-17
Task 3b: Deinstall the Old STA Version—Upgrades From STA 2.0.x or Higher	8-17
Task 4: Install the New STA Version	8-18
Task 5: Dump the New STA Database (optional)	8-19
Task 6: Transfer the Old STA Database to the STA Server	8-20
Task 7: Process and Load the Old STA Database	8-20
Task 8: Upgrade the Old Database	8-22
Recover a Failed Database Upgrade (optional)	8-23
Post-upgrade Tasks for All Upgrades	8-24
Update the STA Trap Recipient on the Libraries	8-24
Configure SNMP Settings in STA	8-25
Configure STA Services and User Information	8-26
Decommission the Old STA Server (optional)	8-26

9 Deinstalling and Restoring STA

STA Deinstallation Overview	9-1
STA Deinstallation Tasks	9-1
Deinstall STA	9-2
Verify Successful Deinstallation	9-2
Restore STA	9-3

A STA Graphical Installer and Deinstaller Screen Reference

Graphical-mode Display Requirements	A-1
Local Connections	A-1
Remote Connections Using a Secure Shell (SSH)	A-2
Remote Connections Using Desktop Sharing	A-2
Troubleshooting Graphical Display Issues	A-3
STA Graphical Installer Screens	A-3
Installation and Inventory Setup	A-5
Welcome	A-6
Installation Location	A-8
Prerequisite Checks	A-10
Enter Root Password	A-14
Set Up DB Directories	A-15
Set Up Admin Accounts	A-16

WebLogic Administrator	A-17
STA Administrator.....	A-18
Set Up Database Accounts.....	A-19
Database Root User.....	A-20
Database Application User	A-21
Database Reports User	A-22
Database Administrator	A-23
Enter Communication Ports	A-24
WebLogic Admin Console.....	A-25
STA Engine.....	A-26
STA Adapter	A-27
STA UI.....	A-28
Diagnostic Agent.....	A-29
Installation Summary	A-30
Installation Progress	A-31
Configuration Progress	A-33
Installation Complete	A-35
STA Graphical Deinstaller Screens	A-35
Welcome	A-36
Enter Root Password	A-37
Deinstallation Summary	A-38
Deinstallation Progress.....	A-39
Deinstallation Complete.....	A-41

B STA Silent-mode Installer and Deinstaller

Using the STA Silent-mode Installer and Deinstaller	B-1
Silent Mode Requirements	B-1
Files and Utilities Used With Silent Mode	B-1
Silent Mode Process	B-2
Silent Mode Tasks.....	B-3
Start the Response File Build Utility	B-4
Create a Response File With Values	B-4
Create an Empty Response File.....	B-8
Add or Modify Clear-text Values in an Existing Response File.....	B-10
Add or Modify Encrypted Passwords in an Existing Response File.....	B-10
Run the Silent-mode Installer.....	B-13
Run the Silent-mode Deinstaller	B-15
Response File Reference Information	B-16
Response File Build Utility Options	B-16
Response File Utility Prompts and File Parameters.....	B-17
Sample Response Files.....	B-18
STA Installer and Deinstaller Command Options	B-20
Silent-mode Options	B-20
Logging Options.....	B-21
Other Options	B-21

C Installation and Upgrade Worksheets

Upgrade Preparation Worksheet	C-1
Installation and Upgrade Worksheets	C-2
Installation Users and Locations Worksheet.....	C-2
User Accounts Worksheet.....	C-3
Port Number Worksheets	C-3
Domain Name Worksheet	C-4
Post-installation Configuration Worksheet	C-5

D Configuring Security Certificates

Security Certificate Configuration Tasks	D-1
Establish the Initial HTTPS/SSL Connection	D-1
Reconfigure WebLogic to use a Different Security Certificate	D-2
Replace the Oracle Certificate	D-9

E Configuring External Authentication Providers for STA

Understanding the WebLogic Server Active Security Realm	E-1
Considerations for Configuring External Authentication Providers	E-2
Supported Authentication Provider Types	E-2
Using the WebLogic Administration Console	E-2
LDAP Principal User	E-2
STA Access Group	E-3
Default STA User Role.....	E-3
Configuring the Authentication Process for Multiple Providers.....	E-3
LDAP Authentication Referrals	E-3
Using SSL for Communications	E-4
Authentication Provider Configuration Process Overview	E-4
Tasks for Configuring Active Directory and OpenLDAP Authentication Providers	E-4
Prepare the External Authentication Provider for STA Authentication.....	E-5
Edit the WebLogic Server Active Security Realm	E-5
Task 1: Add an External Authentication Provider	E-8
Task 2: Define Provider-specific Information	E-10
Task 3: Set the JAAS Control Flag.....	E-15
Task 4: Ensure Proper Order of Authentication Providers.....	E-17
Task 5: Apply All Configuration Changes	E-19
Verify Configuration of Authentication Providers	E-21
Tasks for Configuring IBM RACF Authentication Providers	E-23
Task 1: Review IBM RACF Mainframe Minimum Requirements	E-23
Task 2: Enable Mainframe Support for STA RACF Authorization.....	E-23
Task 3: Configure AT-TLS	E-24
Task 4: Create the RACF Profiles Used by the CGI Routine.....	E-29
Task 5: Import the Certificate File and Private Key File (optional)	E-29
Task 6: Test the CGI Routine	E-29
Task 7: Set Up RACF/SSP for the WebLogic Console.....	E-30
Task 8: Configure SSL Between STA and RACF	E-30
Task 9: Configure the WebLogic Server.....	E-31

Task 10: Install RACF/SSP on the WebLogic Console	E-31
---	------

F Configuring SNMP v2c Mode

When to Use SNMP v2c Mode.....	F-1
SNMP v2c Mode Configuration Process	F-1
SNMP v2c Configuration Tasks	F-1
Create the STA SNMP v2c Trap Recipient on the Library.....	F-2
Enable SNMP v2c Mode for STA.....	F-3

Index

Preface

This document provides concepts and procedures for installing and configuring Oracle's StorageTek Tape Analytics (STA).

Audience

This document is intended for the following audiences:

- Linux Administrator: Installs, configures, and administers Linux on the STA server.
- STA Administrator: Installs, configures, and administers the STA application.
- Library Administrator: Configures and administers StorageTek libraries.
- MVS System Programmer: Configures and administers access to STA by IBM mainframe users.

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 Documents

The STA documentation set consists of the following documents.

For users of the STA application

- *STA Quick Start Guide*—Use this guide to introduce yourself to the STA application and some features of the user interface.
- *STA User's Guide*—Use this guide for instructions on using all STA application features, including the Dashboard, templates, filters, alerts, Executive Reports, logical groups, and STA media validation. This guide also provides instructions for administering and managing STA usernames, email addresses, service logs, and SNMP connections with the monitored libraries.

- *STA Screen Basics Guide*—Use this guide for full details about the STA user interface. It describes the screen navigation and layout, and the use of graphs and tables.
- *STA Data Reference Guide*—Use this guide to look up definitions for all STA tape library system screens and data attributes.

For installers and administrators of the STA server and application

- *STA Release Notes*—Read this document before installing and using STA. It contains important release information, including known issues. This document is included in the STA media pack download.
- *STA Requirements Guide*—Use this guide to learn about minimum and recommended requirements for using STA. This guide includes the following requirements: library, drive, server, user interface, STA media validation, and IBM RACF access control.
- *STA Installation and Configuration Guide*—Use this guide to plan for installation of STA, install the Linux operating system, install the STA application, and then configure STA to begin monitoring the libraries. This guide also provides instructions for upgrading to a new version of STA.
- *STA Administration Guide*—Use this guide for information about STA server administration tasks, such as STA services configuration, database backup and restore, and password administration for database accounts.
- *STA Security Guide*—Read this document for important STA security information, including requirements, recommendations, and general security principles.
- *STA Licensing Information User Manual*—Read this document for information about use of third-party technology distributed with the STA product.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New

This section summarizes new and enhanced features for StorageTek Tape Analytics 2.2.0.

STA 2.2.0 February 2016

Oracle recommends upgrading to STA 2.2.0 or higher to take advantage of the new features described below.

- Maintenance fixes
- Performance improvements
- Updated recommended library and drive requirements to support STA 2.2.0 and higher. See the *STA Requirements Guide* for details.
- New response file build utility for the silent installer and deinstaller. The utility prompts you for the necessary information and saves the response file and an encryption key file to the directory of your choice. It writes passwords to the file in encrypted form. See the *STA Installation and Configuration Guide* for details.

Pre-installation Planning

This chapter includes the following sections:

- [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, perform the following activities in the order listed. You can perform the process yourself or purchase Oracle installation services.

Note: To upgrade STA from a previous version, see [Chapter 8, "Upgrading to STA 2.2.x"](#).

1. Review and verify STA requirements at your site. See the *STA Requirements Guide*.
2. Review installation and configuration best practices. See "[Best Practices for STA Deployment](#)" on page 1-2.
3. Prepare service requests for the drives and libraries, as necessary. See "[Prepare Service Requests for the Libraries and Drives](#)" on page 1-5.
4. Install Linux on the STA server. See "[Installing Linux](#)" on page 2-1.
5. Install STA on the STA server. See "[Installing STA](#)" on page 3-1.
6. Configure the libraries to send data to STA. See "[Configuring SNMP on the Libraries](#)" on page 5-1.
7. Configure STA to receive data from the libraries and begin monitoring. See "[Configuring Library Connections in STA](#)" on page 6-1.
8. Configure additional STA usernames and email addresses. See the *STA User's Guide*.
9. Configure STA monitoring and database backup services. See "[Configuring STA Services](#)" on page 7-1.
10. Configure one or more approved security certificates (optional). See "[Configuring Security Certificates](#)" on page D-1.
11. Configure one or more external providers for STA access control (optional). See "[Configuring External Authentication Providers for STA](#)" on page E-1.

Best Practices for STA Deployment

This section provides tips for optimizing the performance and value of the STA server, database, and application.

Preparation

Dedicated STA server

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

Assistance with STA server sizing

As soon as possible in the planning process, 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 the *STA Requirements Guide*.

Sizing considerations for larger installations

If you have significant exchanges-per-hour rates (that is, greater than 300 EPH), with multiple libraries attached to a single STA server and a long history with STA, you should carefully consider the size and configuration 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 100GB, but you should allocate 200GB if `/tmp` is in the root partition. Allocate another 200GB 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 250GB up to 500GB.
- STA database backups (for example, `/dbbackup`)—Oracle recommends this to be on its own appropriately sized HDD. Guidance is from 500GB up to 2TB.

You may also want to consider using SSDs.

Filesystem layout

For optimal performance and functionality of the STA application, plan your STA filesystem layout and space allocations carefully. The file system is configured during Linux installation.

See "[Review STA File System Layout](#)" on page 2-2.

Linux Installation

Firewalls

For optimal system performance, you may want to disable the firewall on the STA server.

See "[Disable the Linux Firewall](#)" on page 2-8.

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 ["Ensure Proper Setup of yum \(optional\)"](#) on page 2-10.

STA Installation

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 ["Installing STA"](#) on page 3-1.

Oracle central inventory registration

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 STA installation is complete, 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 STA upgrades in the future.

See ["Register the Oracle Central Inventory Location"](#) on page 3-19.

Browser usage 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 \(optional\)"](#) on page 2-13.

Library Configuration for STA

Library and drive firmware levels

To ensure richer library and drive data, use the most current library and drive firmware levels. See the following sections:

- *STA Requirements Guide*, for library firmware requirements
- *STA Requirements Guide*, for drive firmware requirements

Important library configuration steps

To ensure complete compatibility with STA, some library parameters must be set to specific values. Be sure to make the following changes before you configure the library connection to STA so the libraries send data to STA in the correct format.

- For SL8500 libraries, make sure the complex ID is unique for each monitored SL8500 complex.
See ["Ensure the Correct Library Complex ID \(SL8500 only\)"](#) on page 4-9.
- For SL150 and SL500 libraries, ensure the volume label format is set correctly.
See ["Set the SL500 Volume Label Format \(SL500 only\)"](#) on page 4-10.

Quiesce the libraries before changing library parameters

It is recommended that you quiesce all activity to a library before changing its parameters. In addition, tape applications and hosts may require configuration changes after library parameters have been changed.

See ["Set the SL500 Volume Label Format \(SL500 only\)"](#) on page 4-10.

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 ["Duplicate Volume Serial Numbers"](#) on page 4-5.

SNMP Connections With the Libraries

SNMP version

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

See ["Understanding Library SNMP Configuration for STA"](#) on page 5-1.

SNMP v3 user

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

See ["Unique SNMP v3 User"](#) on page 5-2.

Data Collections

Connection testing

Certain activities performed in STA or on a monitored library may cause the SNMP connection with the affected library to be dropped. To minimize the dropped connection time and prevent the loss of large amounts of SNMP data, you should perform a connection test at the following times:

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

See the *STA User's Guide*.

Initial library data collections (MIB walks)

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 quiesced.

See the *STA User's Guide*.

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.

See the *STA User's Guide*.

As-needed data collections

For STA to receive SNMP data from a library, you must perform a manual data collection at the following times:

- After a new library connection has been configured
- After SNMP 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

See the *STA User's Guide*.

STA Services Configuration

Database backups

You should configure a remote backup server for STA database backups.

See "[Configure the Remote Database Backup Server](#)" on page 7-3.

Database backup space management

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 "[Configure the STA Resource Monitor](#)" on page 7-7.

STA Database Tuning

Database considerations for larger installations

If you have significant exchanges per hour rates (that is, greater than 300 EPH) 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.

Parameter	Minimum Recommended Value	Comments
<code>innodb_buffer_pool_size</code>	24 GB or greater	The value should be 70–80 percent of the STA server's physical memory.
<code>innodb_buffer_pool_instances</code>	8	More buffer pools improve concurrent processing.

Prepare Service Requests for the Libraries and Drives

Use this procedure and the referenced sections to provide Oracle Support with the information needed to prepare your libraries and drives for monitoring by STA.

Note: 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.

1. Verify the library firmware version. See ["Verify the Library Firmware Version"](#) on page 4-7.
2. Verify a high-memory HBT card is installed (SL3000 and SL8500 only). See ["Verify the Drive Controller Card Version \(SL3000 and SL8500 only\)"](#) on page 4-8.
3. Enable ADI on library and LTO drives: For libraries with LTO drives only. See ["Enable ADI on the Library \(all libraries except SL150\)"](#) on page 4-9
4. Set the library complex ID (SL8500 only). See ["Ensure the Correct Library Complex ID \(SL8500 only\)"](#) on page 4-9.
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.

Installing Linux

This chapter includes the following topics:

- [Linux Installation Process](#)
- [Preparation Tasks](#)
- [Installation Tasks](#)
- [Post-Installation Tasks](#)

Before installing Linux on the STA server, review the system requirements in the *STA Requirements Guide*.

Note: You cannot perform an in-place upgrade of Linux 5.x to Linux 6.x. If you are installing Linux 6.x as part of an upgrade to STA 2.0.x, see [Chapter 8, "Upgrading to STA 2.2.x."](#)

Linux Installation Process

To install and configure Linux for STA, perform the following tasks in the following sections, in the order indicated.

Preparation

1. ["Review Related Documentation"](#) on page 2-2
2. ["Review STA File System Layout"](#) on page 2-2
3. ["Download the Linux Installer Media Pack"](#) on page 2-3

Installation

1. ["Gather Required Information"](#) on page 2-4
2. ["Install Linux"](#) on page 2-4
3. ["Run the Linux Setup Agent"](#) on page 2-6

Post-installation

1. ["Ensure the Correct root User Path"](#) on page 2-8
2. ["Disable the Linux Firewall"](#) on page 2-8
3. ["Disable SELinux"](#) on page 2-9
4. ["Remove SELinux Permissions"](#) on page 2-9
5. ["Set Up the Network Proxy"](#) on page 2-10
6. ["Ensure Proper Setup of yum \(optional\)"](#) on page 2-10

7. ["Install Required Linux Packages"](#) on page 2-11
8. ["Ensure Proper Setup of SSH"](#) on page 2-12
9. ["Ensure Proper DNS Settings"](#) on page 2-12
10. ["Disable Name Services"](#) on page 2-12
11. ["Ensure Local Browser Functionality \(optional\)"](#) on page 2-13

Preparation Tasks

Before installing Linux on the STA server, perform the procedures in the following sections.

- ["Review Related Documentation"](#) on page 2-2
- ["Review STA File System Layout"](#) on page 2-2
- ["Download the Linux Installer Media Pack"](#) on page 2-3

Review Related Documentation

Due to the wide variety of network configuration requirements and options, refer to the following documents for help with installing and configuring the hardware, software, and network. IPv4 and IPv6 network configuration are discussed in detail in these documents.

- Oracle Linux Installation Guides:
<http://docs.oracle.com/en/operating-systems/>
- RedHat Linux Documentation:
<https://access.redhat.com>

Review STA File System Layout

[Table 2-1](#) describes the recommended file system layout for the STA server. You configure the layout during Linux installation.

The following locations are user-defined, meaning you can configure the layout to meet your site requirements.

- Oracle storage home—The STA installer will prompt you for this location. There is no default. See ["Oracle storage home location"](#) on page 3-2 for details.
- STA database—The STA installer will prompt you for this location. The default is /dbdata.
- STA database local backup—The STA installer will prompt you for this location. The default is /dbbackup.
- STA and MySQL logs—The default is /var/log/tbi. If you want to use a different location, you must create a symbolic link from your desired location to /var/log/tbi after STA has been installed. See ["Relocate the STA Logs Directory \(optional\)"](#) on page 3-18 for instructions.

Oracle recommends creating all these file systems before installing STA; otherwise, STA will be installed in the root "/" and /var directories, requiring additional space allocation to these directories. While the STA installer creates directories as needed, you have greater control of file system properties if you create the files systems in advance.

Note: Oracle recommends that usage for any partition should never exceed 80 percent. Once STA is installed, you can configure the STA Resource Monitor to monitor some locations and automatically notify you if usage exceeds the high-water marks you define. See "[Configure the STA Resource Monitor](#)" on page 7-7 for instructions. You will need to periodically check locations not monitored by the STA Resource Monitor.

Table 2–1 Recommended File System Layout

File System	Default Mount Point	Size	Description and Recommendations
root	/	32 GB minimum	If /tmp is included in this file system, a minimum of 4 GB of free space should be maintained; this space is required during STA installations and upgrades.
swap	None. Defined as memory.	50 to 100 percent of RAM size	Used for swap space.
Oracle storage home	/Oracle	30 GB minimum 50 GB recommended	Location of the STA and Oracle Middleware (WebLogic, MySQL, RDA) application files. This location is user-defined. It 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: <ul style="list-style-type: none"> ▪ 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 it be on a different volume from the STA database, and on mirrored or striped drives in case of database corruption or failure.
STA logs location	/var/log/tbi	30 GB minimum 50 GB to 100 GB recommended	Location of STA and MySQL logs. This location should be a separate volume at a separate mount point. The contents tend to grow and are managed through log rotation. 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) " on page 3-18 for instructions. Note: Except for log rotation, STA does not perform space management. Caution: You must configure the STA backup utility to manage the log files in /STA_logs/db/stadb_bin.*. Otherwise, these files may require manual management (see the <i>STA Administration Guide</i> for details).

Download the Linux Installer Media Pack

Use this procedure to download the Linux installer media pack from the Oracle Software Delivery Cloud website. The media pack is delivered as a compressed ISO

image file, which you can extract and write to portable media of your choice (flash drive, DVD, etc.).

Before performing this task, you must obtain an Oracle Software Delivery Cloud user ID and password from your Oracle support representative.

1. Start a Web browser and navigate to the Oracle Software Delivery Cloud website:
<http://edelivery.oracle.com/linux>
2. Click **Sign In/Register**.
3. Enter the user ID and password provided by Oracle Support.
4. On the Terms & Restrictions screen, select the boxes to indicate your acceptance of the License Agreement and Export Restrictions, and then click **Continue**.
5. On the Media Pack Search screen:
 - a. In the Select a Product Pack menu, select **Oracle Linux**.
 - b. In the Platform menu, select **x86 64 bit** (STA requires 64-bit Linux).
 - c. Click **Go**.
6. Select a Linux version, and then click **Continue**.
For Linux version requirements, see the *STA Requirements Guide*.
7. Click **Download** for the 64-bit option.
8. Save the ISO file and write it to media.

Installation Tasks

To install Linux on the STA server, perform the procedures in the following sections.

- "[Gather Required Information](#)" on page 2-4
- "[Install Linux](#)" on page 2-4
- "[Run the Linux Setup Agent](#)" on page 2-6

Note: These procedures assume an Oracle Enterprise Linux (OEL) 6u4 DVD installation with graphical installer and setup agent. If you install a different version of Linux, use different media, or use the console mode, the steps and packages may vary.

Gather Required Information

Contact your system administrator to obtain the following 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

Install Linux

Use this procedure to perform the Linux installation.

1. Connect the installation media to the STA server.
2. Start the Linux installer using the instructions in the README file on the media.
3. Select **Install or upgrade an existing system**.
4. 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**.
5. On the Welcome screen, click **Next**.
6. Select a language, and then click **Next**.
7. Select a keyboard layout, and then click **Next**.
8. Select **Basic Storage Devices**, and then click **Next**.
9. Enter a hostname for the STA server, and then click **Configure Network**.
10. Select the network adapter name, and then click **Edit**.
11. Ensure that **Connect automatically** and **Available to all users** are both selected.
12. 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**.
13. Select the STA server's time zone, select the **System clock uses UTC** check box, and then click **Next**.
14. Enter and confirm a Linux root password for the server, and then click **Next**.
15. Identify a partitioning layout to use on the server:
 - a. Because STA requires a dedicated server, Oracle recommends selecting **Use All Space**.
 - b. Select the **Review and modify partitioning layout** check box, and then click **Next**.
16. Use [Table 2-1](#) 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**.
17. When ready, select **Write changes to disk**.
18. In the boot loader screen, leave all options as-is, and then click **Next**.
19. In the software selection screen, select **Basic Server**, and do not change the repository options. Then, select **Customize now**, and then click **Next**.
20. In the package selection screen, use [Table 2-2](#) to configure the packages for each package category:
 - a. Select a package category.
 - b. Select the box for each package in the Select column.
 - c. 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**.
 - d. Deselect the box for each package in the Deselect column.
 - e. Leave other check boxes as-is.

Table 2–2 Linux Package Selection

Package Category	Select	Deselect
Base System	<ul style="list-style-type: none"> ■ Base ■ Compatibility libraries ■ Console internet tools ■ Java Platform ■ Legacy UNIX compatibility + ksh-xxxxxxx-xx.el6.x86_64 	<ul style="list-style-type: none"> ■ Debugging Tools ■ Dial-up Networking Support ■ Directory Client ■ Hardware monitoring utilities ■ Large Systems Performance ■ Network file system client ■ Performance Tools
Servers (optional)	<ul style="list-style-type: none"> ■ 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 "Post-Installation Tasks" on page 2-7 for details.	<ul style="list-style-type: none"> ■ Desktop ■ Desktop Platform ■ General Purpose Desktop + system-config-lvm-x.x.xx-xx.el6.noarch¹ ■ Legacy X Window System compatibility ■ X11 (X Window System, version 11) 	NA
Applications (optional)— Can be used to configure and manage the STA server locally with the GUI interface.	<ul style="list-style-type: none"> ■ Internet Browser 	NA
Development	<ul style="list-style-type: none"> ■ Development tools + expect-x.xx.x.xx-x.el6.x86_64 	NA
Languages	NA	NA

¹ Optional. Can be used to configure or re-configure the file system once Linux installation is complete.

21. 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.

22. 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 Linux server. Use this procedure 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 root user:
 - a. Click **Other...**
 - b. Enter username **root**, and then click **Log In**.
 - c. Enter the root password, and then click **Log In** again.
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
Oracle Linux Server release 6.4
Red Hat Enterprise Linux Server release 6.4 (Santiago)
Oracle Linux Server release 6.4
```

Post-Installation Tasks

To ensure that the STA server is configured properly for STA installation, perform the tasks in the following sections.

- ["Ensure the Correct root User Path"](#) on page 2-8
- ["Disable the Linux Firewall"](#) on page 2-8
- ["Disable SELinux"](#) on page 2-9
- ["Remove SELinux Permissions"](#) on page 2-9
- ["Set Up the Network Proxy"](#) on page 2-10
- ["Ensure Proper Setup of yum \(optional\)"](#) on page 2-10
- ["Install Required Linux Packages"](#) on page 2-11
- ["Ensure Proper Setup of SSH"](#) on page 2-12

- ["Ensure Proper DNS Settings"](#) on page 2-12
- ["Disable Name Services"](#) on page 2-12
- ["Ensure Local Browser Functionality \(optional\)"](#) on page 2-13

Ensure the Correct root User Path

Use this procedure to ensure that the necessary directories for Linux configuration are included in the path for the system root user.

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 back 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
```

Disable the Linux Firewall

For optimal system performance, Oracle recommends disabling the firewall on the STA server. However, you may choose to enable and configure the firewall depending on your site requirements.

Use this procedure to disable the firewall.

1. Check the settings of the Linux firewall (for next boot).

```
# chkconfig --list | grep "ip"
```

If the firewall is set to be disabled on next boot, all output for both iptables and ip6tables will show as off. If this is not the case, disable the firewall.

```
# chkconfig iptables off
# chkconfig ip6tables off
```

2. Check the current status of the Linux firewall.

```
# service iptables status
```

```
# service iptables status
```

The command output will indicate if the firewall is currently running. If the firewall is running, stop the firewall.

```
# service iptables stop
# service ip6tables stop
```

Disable SELinux

STA does not support SELinux. You must use this procedure to 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

Use this procedure to remove SELinux permissions for directories that were created before you disabled SELinux. 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. 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

You can 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**.

Ensure Proper Setup of yum (optional)

There are a variety of methods for installing the required RPM (Red Hat Package Manager) Linux software packages. Oracle recommends you use yum (Yellowdog Updater, Modified), as it greatly simplifies the package installation process. yum automatically searches RPM package repositories for the latest package versions and their dependencies. See "[Install Required Linux Packages](#)" on page 2-11 for the required packages.

If you will be using yum, use this procedure to ensure that yum is configured correctly on the STA server.

Note: The following command examples use the yum repository for Oracle Linux. In the commands, the "l" in "ol6" is lowercase "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-ol6.repo
```

3. Remove the existing yum repository file.

```
# rm public-yum-ol6.repo
```

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

```
# wget http://public-yum.oracle.com/public-yum-ol6.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-ol6.repo.1). However, yum always uses the repository file with no extension.

5. Open the repository file with a text editor.

```
# vi public-yum-ol6.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/OL6/x/base/$basearch/
gpgkey=http://public-yum.oracle.com/RPM-GPG-KEY-oracle-ol6
gpgcheck=1
enabled=1
```

7. Save and exit the file.

Install Required Linux Packages

Additional RPM packages are required for STA installation and operation. The STA installer will check for the following packages and if they are not present, STA installation will fail.

Note: RPM package names are case-sensitive.

<input type="checkbox"/> binutils	<input type="checkbox"/> gcc-c++	<input type="checkbox"/> libstdc++
<input type="checkbox"/> compat-libcap1	<input type="checkbox"/> glibc	<input type="checkbox"/> libstdc++-devel
<input type="checkbox"/> compat-libstdc++-33.i686	<input type="checkbox"/> glibc-devel	<input type="checkbox"/> net-snmp-utils
<input type="checkbox"/> cronic	<input type="checkbox"/> libaio	<input type="checkbox"/> rpm-build
<input type="checkbox"/> expect	<input type="checkbox"/> libaio-devel	<input type="checkbox"/> sysstat
<input type="checkbox"/> gcc	<input type="checkbox"/> libgcc	<input type="checkbox"/> xorg-x11-utils

You can use a variety of methods to install the required RPM packages. This procedure describes how to use yum.

The yum package install command checks for the most current version of the package for your Linux 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. Proceed as follows:
 - If you can reach Oracle's public yum server (see "[Ensure Proper Setup of yum \(optional\)](#)" on page 2-10), 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 binutils compat-libcap1 compat-libstdc++-33.i686
cronie expect gcc gcc-c++ glibc glibc-devel libaio libaio-devel libgcc
libstdc++ libstdc++-devel net-snmp-utils rpm-build sysstat
xorg-x11-utils
```

- 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
```

Ensure Proper Setup of SSH

Use this procedure to ensure that SSH (secure shell) is set up correctly 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.

```
# service sshd restart
```

Ensure Proper DNS Settings

Use this procedure to ensure that the STA server's IP address is mapped 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. Use this procedure to temporarily disable these services.

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 (see the *STA Requirements Guide*).

If STA is accessed at your site using the HTTPS protocol, see the *STA User's Guide* for instructions on ensuring that HTTPS is supported by your browser.

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

Installing STA

This chapter assumes you are performing a new installation of STA on this server. Only one instance of STA can be installed on the server.

- If you are upgrading STA from a previous version, see [Chapter 8, "Upgrading to STA 2.2.x"](#). Oracle recommends you install or upgrade to the latest version of STA.
- If you need to reinstall STA or repair a current installation, see [Chapter 9, "Deinstalling and Restoring STA."](#)

Note: Oracle provides support only if STA is installed on a dedicated server (called the *STA server*).

This chapter includes the following topics:

- [Users, Groups, and Locations Used by the STA Installer](#)
- [Username and Password Requirements](#)
- [Accounts and Ports Configured During STA Installation](#)
- [STA Installation and Deinstallation Logs](#)
- [STA Installer Modes](#)
- [STA Installation Tasks](#)

[Appendix C](#) includes worksheets you can use to organize your installation activities and record your settings.

Users, Groups, and Locations Used by the STA Installer

This section describes key concepts and terms used in the STA installation process.

Oracle install group

A 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 the STA installation, 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; substitute the name you have chosen if it is different.

Oracle install user

A Linux user for installing and upgrading Oracle products on the STA server. This can be any user that is a member of the Oracle install group.

The instructions and examples in this guide use the name `oracle` for this user; substitute the name you have chosen if it is different.

Oracle central inventory location

The directory used for tracking information about Oracle products installed on the STA server. STA installer and deinstaller logs are kept in the `logs` subdirectory within this location.

The Oracle install user must own this directory and have full permissions to it. To ensure other users in the Oracle install group have proper access so they can install Oracle products, you should not use the Oracle install user's home directory.

This location should be separate from the other directories described in this section. The instructions and examples in this guide use `/opt/oracle/orainventory` for this location; substitute the directory you have chosen if it is different.

Note: Oracle recommends registering this location after STA installation is complete so all Oracle installers use the same central inventory location on this server. See "[Register the Oracle Central Inventory Location](#)" on page 3-19 for details.

Oracle storage home location

The directory where STA and associated Oracle software are installed. STA is automatically installed in the `StorageTek_Tape_Analytics` subdirectory within this location; see "[STA home](#)".

This directory must be owned by the Oracle install group, not `root`, and the Oracle install user must have full permissions to it. If this directory does not exist, the STA installer will automatically create it if the Oracle install user has full permissions to the parent directory.

Note: If an earlier version of STA was installed on this server, this directory may already exist. If so, you should verify the correct ownership and permissions.

This location should be separate from the other directories described in this section. The instructions and examples in this guide use `/Oracle` for this location; substitute the directory you have chosen if it is different.

STA home

The directory where all STA software is installed. This directory is assigned the name `StorageTek_Tape_Analytics`, and the STA installer automatically creates it within the "[Oracle storage home location](#)".

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.

This location should be separate from the other directories described in this section. The instructions and examples in this guide use `/Installers` for this location; substitute the directory you have chosen if it is different.

STA installer working location

By default, the STA and WebLogic installer files are unpacked to the `STA_home/tmp` directory, which requires a minimum 11 GB of space. You can have the STA installer files unpacked to a different working location by running the STA installer with the following option: `-J-Djava.io.tmpdir=working_directory`

`working_directory` must be an absolute path. For example:

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

See "[STA Silent-mode Installer and Deinstaller](#)" on page B-1 for details about using this option.

STA logs location

Location of the STA and MySQL logs. The contents tend to grow and are managed through log rotation. 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 \(optional\)](#)" on page 3-18 for instructions.

See "[Review STA File System Layout](#)" on page 2-2 for space requirements.

Username and Password Requirements

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:

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

Accounts and Ports Configured During STA Installation

The STA installer configures user accounts and port numbers according to the specifications you provide.

User Accounts for Managing STA

The following required accounts are created during STA installation. These accounts are specific to STA, and they are *not* Linux usernames.

- [WebLogic Accounts](#)
- [STA Database Accounts](#)

WebLogic Accounts

The following WebLogic accounts are used to log in to the WebLogic administration console or the STA application.

WebLogic Administration

Use to log in to the WebLogic administration console to make changes to the WebLogic environment—for example, to connect WebLogic to an LDAP or RACF server.

Caution: The username and password for this account are not retrievable. If these credentials are lost, STA must be re-installed.

STA Administrator

Use to log in to the STA application with full access privileges.

After the STA installation has been completed, you can use the STA application to create additional user accounts with assignable roles; see the *STA User's Guide* for details.

STA Database Accounts

The following STA database accounts are MySQL accounts used by STA to access and manage the STA database.

STA Database Root User

Owns the MySQL database and is used to create the root database installation. The predefined username is `root`, and it cannot be changed.

Caution: The password for this account is not retrievable.

STA Database Application User

A user-defined MySQL username (for example, `stadb`) that STA uses to connect to the database. It is required to create, update, delete, and read privileges on data tables.

STA Database Reports User

A user-defined MySQL username (for example, `stardt`) that non-STA and third-party applications may use to connect to the database. It has read-only access to certain database tables.

STA Database Administrator User

A user-defined MySQL username (for example, `stadba`) that STA administration and monitoring utilities use to connect to the database, primarily to configure and run scheduled backups. It has all DBA privileges except the "grant option" on all database tables.

Ports Used by STA

STA uses the following ports to retrieve and receive data. These are dedicated ports, and they must remain available to STA. The STA installer will verify that the ports are not already in use on the network.

Caution: Once these ports have been configured during STA installation, they cannot be changed without deinstalling and reinstalling STA.

Unconfigurable External Ports

The ports described in [Table 3-1](#) are external ports used for communication between the STA server and other network entities. The port values are fixed and cannot be changed during STA installation.

Firewall/router configuration: Must be reachable between the STA server and the backup server (for SSH), and between the STA server and the monitored libraries (for SNMP and SNMPTRAP).

Table 3-1 Unconfigurable External Ports

Port	Protocol	Description/Purpose
22	SSH	Secure Shell. STA database backup; library log-in.
161	SNMP	Simple Network Management Protocol (SNMP). For transmittal of SNMP requests.
162	SNMPTRAP	For reception of SNMP notifications (traps).

Configurable External Ports

The ports described in [Table 3-2](#) are external ports used for communication between the STA server and other network entities. These ports are the configurable equivalent of standard ports 80 and 8080 (HTTP) and 443 (HTTPS), and they must be unique from other HTTP and HTTPS ports on the network. Contact your network administrator for assistance in choosing their values.

Firewall/router configuration: Must be reachable between the STA server and the client running the STA GUI.

Table 3-2 Configurable External Ports

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

Configurable Internal Ports

The ports described in [Table 3-3](#) are used for internal STA communications. These port values must be unique.

Firewall/router configuration: Not applicable

Table 3-3 Configurable Internal Ports

Default Port	Protocol	Description/Purpose
7023	HTTP	staEngine managed server. Basic STA internals, unsecure.
7024	HTTPS	staEngine managed server. Basic STA internals, secure.
7025	HTTP	staAdapter managed server. SNMP communication, unsecure.
7026	HTTPS	staAdapter managed server. SNMP communication, secure.

STA Installation and Deinstallation Logs

You can use the STA installation 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 or deinstallation fails. See ["/STA_logs/install"](#) on page 3-6 for details about their location.

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

Log File Locations

The locations of STA installation and deinstallation logs vary depending on the status of the operation. Logs are found in the following directories. See ["Review STA File System Layout"](#) on page 2-2 for details about these directories.

/tmp/OralInstalltimestamp

This directory includes logs for in-progress installations 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.

```
install2014-09-24_04-14-04PM.log
installProfile2014-09-24_04-14-04PM.log
launcher2014-09-24_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 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.

```
2015-08-05_01-55-59PM.log
install2015-08-05_01-55-59PM.log
install2015-08-05_01-55-59PM.out
installActions2015-08-05_01-55-59PM.log
OPatch2015-08-05_01-57-13-PM.log
OPatch2015-08-05_01-59-36-PM.log
oraInstall2015-08-05_01-55-59PM.err
oraInstall2015-08-05_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 \(optional\)"](#) on page 3-18 for instructions.

This directory includes logs for installations 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_install2015-08-05_01-55-51PM.log
dbinstall.log
dbinstall.mysqlld.err
dbinstall.stadb-slow.log
install2015-08-05_01-42-09PM.log
patch_adf.log
sta_install2015-08-05_01-54-04PM.log
weblogic_install2015-08-05_01-55-34PM.log

```

STA Installer Modes

You can install STA using either of the following modes:

Graphical mode

This is the recommended installation mode. This mode provides a graphical user interface for installing STA, and it requires an X11 display. See ["STA Graphical Installer and Deinstaller Screen Reference"](#) for details.

Silent mode

This mode allows you to bypass the graphical user interface and supply the installation options in an XML properties file called the *response file*. See ["STA Silent-mode Installer and Deinstaller"](#) on page B-1 for details.

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 Installation Tasks

To install STA, perform all the following tasks in the order listed.

1. ["Identify or Create Information Required for the Installation"](#) on page 3-7
2. ["Verify Installation Prerequisites"](#) on page 3-9
3. ["Download STA"](#) on page 3-11
4. ["Install STA"](#) on page 3-16
5. ["Verify Successful Installation"](#) on page 3-17
6. ["Relocate the STA Logs Directory \(optional\)"](#) on page 3-18
7. ["Register the Oracle Central Inventory Location"](#) on page 3-19

Identify or Create Information Required for the Installation

Use this procedure to identify and, if necessary, create users and locations to run the STA installer. You can use [Table C-2, "Installation Users and Locations Worksheet"](#) to record this information. See ["Users, Groups, and Locations Used by the STA Installer"](#) on page 3-1 for details about these items.

1. Log in as the system root user.
2. Determine whether there is an Oracle central inventory pointer file, `/etc/orainst.loc`, on the STA server. The file is present if the Oracle central inventory has been registered previously; see ["Oracle central inventory location"](#) on page 3-2 for details.
 - If the file exists, record its contents. For example:

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

The `inventory_loc` entry identifies the Oracle central inventory location, and the `inst_group` entry identifies the Oracle install group.

- If the file is not present, proceed to Step 3 to create the necessary users and locations. For example:

```
# cat /etc/oraInst.loc
cat: /etc/oraInst.loc: No such file or directory
```

3. If there was no Oracle central inventory pointer file in Step 2, create the Oracle install group. See ["Oracle install group"](#) on page 3-1 for details. For example:

```
# groupadd oinstall
```

4. Obtain the username and password of an Oracle install user, or create a new one if necessary. This user must belong to the Oracle install group. See ["Oracle install user"](#) on page 3-2 for details. For example:

```
# useradd -g oinstall -d /home/oracle oracle
# passwd oracle
Changing password for user oracle.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

5. If there was no Oracle central inventory pointer file in Step 2, create the Oracle central inventory location. This directory must be owned by the Oracle install user. See ["Oracle central inventory location"](#) on page 3-2 for details. For example:

```
# mkdir /opt/oracle/oraInventory
# chown oracle /opt/oracle/oraInventory
# chgrp oinstall /opt/oracle/oraInventory
# ls -la /opt/oracle/oraInventory
total 8
drwxr-xr-x 2 oracle oinstall 4096 Feb 11 10:49 .
drwxr-xr-x 3 root   root     4096 Feb 11 10:49 ..
```

6. Locate the Oracle storage home location, or create the directory if it does not exist. This directory must have at least 11 GB of free space and it must be owned by the Oracle install user. See ["Oracle storage home location"](#) on page 3-2 for details. For example:

```
# mkdir /Oracle
# chown oracle /Oracle
# ls -la /Oracle
total 8
drwxr-xr-x 2 oracle oinstall 4096 Feb 11 10:49 .
drwxr-xr-x 3 root   root     4096 Feb 11 10:49 ..
```

7. Locate the STA installer location, or create the directory if it does not exist. See ["STA installer location"](#) on page 3-2 for details. For example:

```
# mkdir /Installers
```

8. Obtain the password for the system root user. The STA installer requires root access to perform certain tasks and will prompt for the password.

9. Choose usernames for the WebLogic Administrator, STA Administrator, and MySQL accounts that will be created during the installation. See ["User Accounts for Managing STA"](#) on page 3-3 for details.
10. 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. See ["Ports Used by STA"](#) on page 3-4 for details.
11. 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

Use this procedure to verify prerequisites before running the STA installer. This procedure is optional, but if any of these prerequisites are not met, the STA installation will fail. See the *STA Requirements Guide* for a complete list of installation requirements.

All these steps are performed on the STA server. Contact your Linux administrator if you need assistance.

Note: STA installation assumes 64-bit Linux has been installed with the Linux RPM packages specified in [Chapter 2, "Installing Linux"](#). 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 the following documents for details:

- The *STA Requirements Guide* for supported Linux versions.
 - ["Install Required Linux Packages"](#) on page 2-11 for a list of required packages
-
-

Caution: Before choosing to permanently remove or replace existing software, back up files as needed.

1. 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 perform a manual post-installation upgrade. See ["Upgrading to STA 2.2.x"](#) on page 8-1 for details.

2. 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.

3. Verify that the /tmp directory has at least 4 GB of free space.

```
$ df -H /tmp
Filesystem                Size      Used Avail Use% Mounted on /dev/mapper/vg_
tbivb03-lv_root
                        53G       35G   16G  70% /
```

4. 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. See ["Oracle storage home location"](#) on page 3-2 for details about this directory.

For example:

```
$ df -H /Oracle
Filesystem                Size      Used Avail Use% Mounted on /dev/mapper/vg_
tbivb03-STA_OracleVol
                        34G       3.8G   29G  12% /Oracle
```

Note: You can optionally specify a different working directory when you start the STA installer. See ["STA installer working location"](#) on page 3-3 for details.

5. Verify SELinux is disabled. If you have followed the instructions in ["Post-Installation Tasks"](#), SELinux should already be disabled; see ["Disable SELinux"](#) on page 2-9 for details.

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

6. Verify Linux firewall (IPTables) is stopped. If you have followed the instructions in ["Post-Installation Tasks"](#), IPTables should already be stopped; see ["Disable the Linux Firewall"](#) on page 2-8 for details.

```
$ service iptables status
iptables: Firewall is not running.
```

Note: If your site requires the IPTables service to be running, you can start the service after you have installed STA, configured the libraries, and confirmed that STA is monitoring the libraries. After starting IPTables, you should reconfirm that STA is monitoring the libraries.

7. Stop and deconfigure SNMP services.

To avoid network port collisions and other issues, the STA server must not be running other SNMP services. The STA installer will quit in either of 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.

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

```
# service snmpd status
snmpd is stopped
# service snmptrapd status
snmptrapd is stopped
```

- b. If necessary, stop the SNMP services immediately.

```
# service snmpd stop
```

```
# service snmptrapd stop
```

Note: If you receive a "FAILED" error with either of these commands, the services may already be stopped.

- c. Type the following to disable the SNMP services in the Linux services configuration file so they do not start automatically when Linux reboots:

```
# chkconfig snmpd off
# chkconfig --list snmpd
snmpd          0:off  1:off  2:off  3:off  4:off  5:off  6:off
# chkconfig snmptrapd off
# chkconfig --list snmptrapd
snmptrapd     0:off  1:off  2:off  3:off  4:off  5:off  6:off
```

8. Review and verify the applicable mode-specific requirements, as follows:
- For the STA graphical installer, see "[Graphical-mode Display Requirements](#)" on page A-1.
 - For the STA silent-mode installer, see "[Silent Mode Requirements](#)" on page B-1.

Download STA

The STA installer download includes the following files. *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 STA silent-mode installer or deinstaller. See [Appendix B, "STA Silent-mode Installer and Deinstaller"](#) for details
1. In a browser window, access the Oracle Software Delivery Cloud website at the following URL:
<http://edelivery.oracle.com/>
 2. Click **Sign In**.



If you do not already have an Oracle account, select the **New User? Register Here** link.

3. Enter the user ID and password provided by Oracle Support.

4. On the Export Restrictions screen, click **Accept**.

ORACLE CLOUD FAQ English Sign Out

Oracle Software Delivery Cloud *To switch to the original Oracle Software Delivery Cloud, click [here](#).*

Export Restrictions

You agree that U.S. export control laws and other applicable export and import laws govern the export, re-export, transfer and use of the programs, including technical data; additional information can be found on [Oracle's Global Trade Compliance website](#).

You agree that neither the programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Oracle Employees:

Under no circumstances are Oracle Employees authorized to download software for the purpose of distributing it to customers. Oracle products are available to employees for internal use or demonstration purposes only. In keeping with Oracle's trade compliance obligations under U.S. and applicable law, failure to comply with this policy could result in disciplinary action up to and including termination.

Decline **Accept**


5. Perform the following steps on the Selected Products screen:
 - a. In the **Product** menu, type **StorageTek Tape**, and then select StorageTek Tape Analytics.
 - b. In the **Select Platform** menu, select the **Linux x86-64** check box and then click **Select**.
 - c. Click **Continue**.

Oracle Software Delivery Cloud *To switch to the original Oracle Software Delivery Cloud, click [here](#).*


To select products for download, enter the Oracle Product into the type-ahead field below, then select from the list of available platforms. Once you have made your selection, the title will be displayed in the 'Selected Products' section below. Repeat this step for all titles you wish to download. Once complete, click on the 'Continue' button. **You must agree to Oracle's trial license terms before downloading products that you do not have a current valid license to use.**

Filter Products By Programs Linux/OVM/VMs Self-Study Courseware 1-Click Offerings

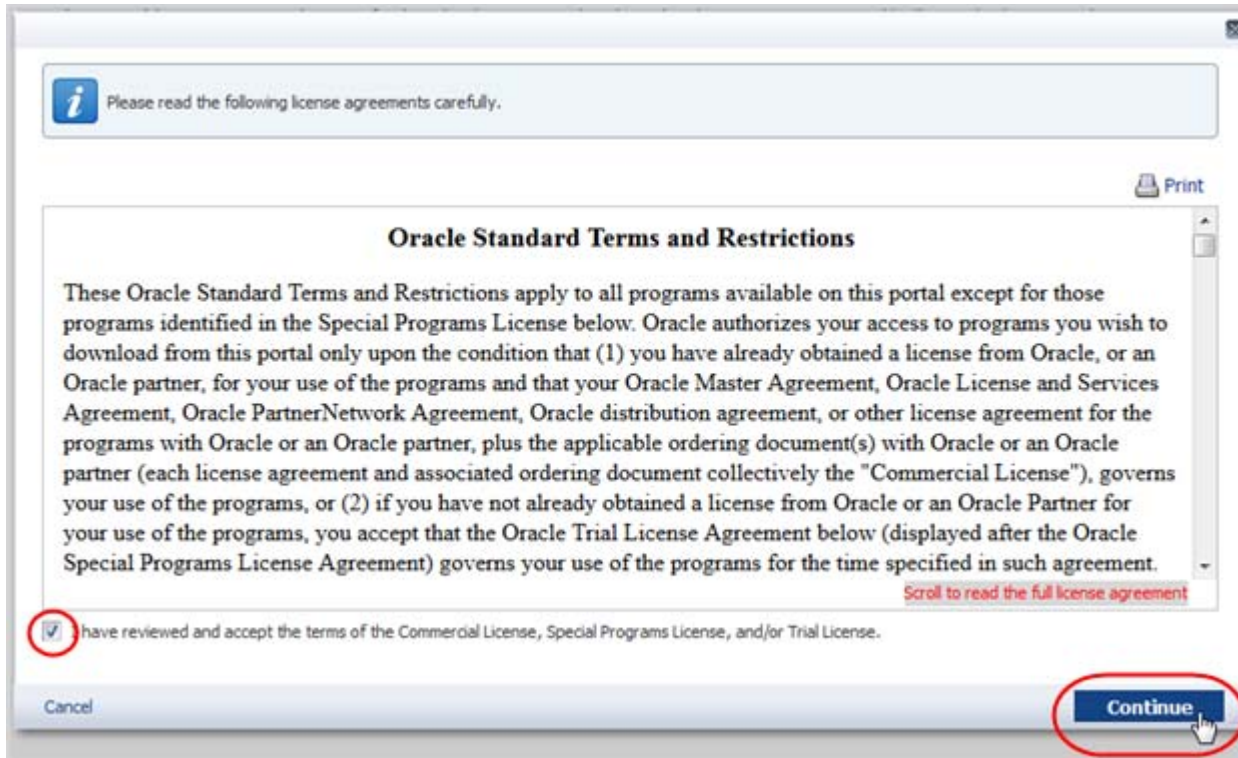
Product *

Selected Products	
Product	Platform
StorageTek Tape Analytics 	Linux x86-64
Quick Select - Select additional products that are often downloaded with these products.	

About Oracle | Legal Notices | Terms of Use | Your Privacy Rights
Copyright © 2015 Oracle and/or its affiliates. All rights reserved.



6. On the Oracle Standard Terms and Restrictions screen, read the terms, select the **I have reviewed and accept the terms...** check box, and then click **Continue**.



- The File Download screen appears, listing the files you have selected. To download all files at once, click **Download All**. To download one file at a time, select the active link with the file name. Save the files to a location containing at least 4 GB of free space.



8. If this is the first time you have used the eDelivery site, the Download Manager dialog box appears. If you have already installed the download manager, you can skip this step.

Select the **Download the installer** link to download the Akamai NetSession Interface download manager. Once installed, the download manager displays the progress of the file downloads in a separate window.



9. Once the download is complete, use an unzip tool or command to extract the zip files to the STA installer location you have selected in "[Identify or Create Information Required for the Installation](#)" on page 3-7 (for example /Installers). For example:

```
# unzip V76699-01_1of2.zip -d /Installers
Archive:  V76699-01_1of2.zip
  inflating: /Installers/V76699-01_1of2.zip
# unzip V76699-01_2of2.zip -d /Installers
Archive:  V76699-01_2of2.zip
  inflating: /Installers/V76699-01_2of2.zip
```

Note: Unzip only the top-level zip files you have downloaded from the eDelivery site (for example, V76699-01of2.zip). Do not unzip any compressed files that are contained within these files (for example, sta_install_2.1.1.9.16_linux64-2.zip).

10. Ensure that the Oracle install 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 the sta_install_version_linux64-2.zip file and silentInstallUtility_version.jar files

By default, the files are owned by the user you were logged in as when you downloaded the files from the Oracle eDelivery site. For example:

```
# cd /Installers
# ls -la
-rw-r--r--  1 root root      5964 Oct 23 16:14 silentInstallUtility_
2.1.0.64.124.jar
-rw-r--r--  1 root root 1275158996 Oct 23 13:35 sta_install_2.1.0.64.124_
linux64-2.zip
-rw-r--r--  1 root root 1599220560 Oct 23 13:01 sta_install_2.1.0.64.124_
linux64.bin
```

```

# chown oracle:oinstall sta_install*.bin
# chmod u+x sta_install*.bin
#
# chown oracle:oinstall sta_install*.zip
# chmod u+r sta_install*.zip
#
# chown oracle:oinstall silentInstallUtility*.jar
# chmod u+r silentInstallUtility*.jar
#
# ls -la
-rw-r--r-- 1 oracle oinstall      5964 Oct 23 16:14 silentInstallUtility_
2.1.0.64.124.jar
-rw-r--r-- 1 oracle oinstall 1275158996 Oct 23 13:35 sta_install_
2.1.0.64.124_linux64-2.zip
-rwxr--r-- 1 oracle oinstall 1599220560 Oct 23 13:01 sta_install_
2.1.0.64.124_linux64.bin

```

11. Review the *STA Release Notes*, which are included in the installer download package.

Install STA

Use this procedure to run the STA installer. You can install STA using either the graphical or silent mode. See "[STA Installer Modes](#)" on page 3-7 for details.

1. In a terminal window, connect to the STA server and log in as the Oracle install user. See "[Oracle install user](#)" on page 3-2 for details.
2. Change to the STA installer location; see "[STA installer location](#)" on page 3-2 for details. For example:

```
$ cd /Installers
```

3. Launch the STA installer with one of the following commands:

- To use the STA graphical installer:

```
$ ./sta_install_version_linux64.bin
```

Where *version* is the version of the STA installer you downloaded. For example:

```
$ ./sta_install_2.1.0.64.124_linux64.bin
```

This mode requires an X11 display. See [Appendix A, "STA Graphical Installer and Deinstaller Screen Reference"](#) for instructions.

- To use the STA silent installer:

```
$ ../sta_install_version_linux64.bin -silent -responseFile response_file
```

Where:

- *version* is the version of the STA installer you downloaded.
- *response_file* is the absolute path of the previously created response file.

For example:

```
$ ./sta_install_2.1.0.64.124_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

Appendix B, "STA Silent-mode Installer and Deinstaller" for instructions.

Verify Successful Installation

Use this procedure to verify that STA is running.

1. Use the following steps to ensure that the STA bin directory is included in the PATH variable for the system root user.

- a. Open a terminal session on the current STA server, and log in as the system root user.
- b. Use a text editor to open the user profile. For example:

```
# vi /root/.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 system root user.
- f. Confirm that the PATH variable has been updated correctly.

```
# echo $PATH
```

```
/usr/lib64/qt-3.3/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin:/Oracle/StorageTek_Tape_Analytics/common/bin
```

2. Use the STA command to verify that all STA services are running and active. [Example 3-1](#) is a sample successful status display. See the *STA Administration Guide* for details.

Example 3-1 STA Successful Status Display

```
$ 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
stai service is running
... and the deployed application for stai 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 [Chapter 5, "Configuring SNMP on the Libraries"](#) and [Chapter 6, "Configuring Library Connections in STA"](#) for instructions.
 - If there are any issues with the STA services, you can review the installation and STA logs for more information. See ["STA Installation and Deinstallation Logs"](#) on page 3-6 for their locations.

Relocate the STA Logs Directory (optional)

Use this procedure only if you want to relocate the STA and MySQL logs to a location other than the default, which is `/var/log/tbi`. After you complete this procedure, new logs will be written to the location you designate. You can perform this procedure anytime after STA has been installed. See ["Review STA File System Layout"](#) on page 2-2 for the location requirements.

1. Log in as the system root user.
2. Stop all STA services.

```
# STA stop all
Stopping the stau service.....
Successfully stopped the stau service
Stopping the staadapter service.....
Successfully stopped the staadapter service
Stopping the staengine service.....
Successfully stopped the staengine service
Stopping the staweblogic service.....
Successfully stopped the staweblogic service
Stopping the staservd Service...
Successfully stopped staservd service
Stopping the mysql service.....
Successfully stopped mysql service
#
```

3. Create the new STA logs directory you want to use for STA and MySQL logs. For example:

```
# mkdir -p /LOGS_DIR/log/
# ls -ld /LOGS_DIR/log
drwxr-xr-x 2 root root 4096 Jan 20 14:17 /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
# ls -ld /LOGS_DIR/log
drwxrwxrwx 2 root root 4096 Jan 20 14:17 /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/
# ls -l /LOGS_DIR/log/tbi
total 20
drwxrwxrwx 2 mysql mysql 4096 Jan 7 10:45 backups
drwxrwxrwx 3 mysql mysql 4096 Jan 7 10:45 db
drwxrwxrwx 2 mysql mysql 4096 Jan 7 11:30 install
-rwxrwxrwx 1 root root 1191 Jan 20 13:04 monitor_staserver.log
drwxrwxrwx 2 root root 4096 Jan 7 11:03 uidumps
```

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
# ls -l /var/log/tbi
lrwxrwxrwx 1 root root 15 Jan 20 14:22 /var/log/tbi -> /LOGS_
DIR/log/tbi
#
```

7. Restart STA.

```
# STA start all
Starting mysql Service..
mysql service was successfully started
Starting staservd Service.
staservd service was successfully started
Starting staweblogic service.....
staweblogic service was successfully started
Starting staengine Service.....
staengine service was successfully started
Starting staadapter Service.....
staadapter service was successfully started
Starting staii Service.....
staii service was successfully started
#
```

Register the Oracle Central Inventory Location

Use this procedure after STA installation has completed to register the Oracle central inventory location on the STA server. You only need to use this procedure once on this server.

This procedure creates an Oracle central inventory pointer file, `/etc/orainst.loc`, which allows the Oracle central inventory location and Oracle install group to be known to all Oracle installers used on the server.

1. Log in as the Linux root user.
2. 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
```

3. Run the registration script, located in that directory.

```
# ./createCentralInventory.sh
Setting the inventory to /opt/oracle/oraInventory
Setting the group name to oinstall
Creating the Oracle inventory pointer file (/etc/orainst.loc)
Changing permissions of /opt/oracle/oraInventory to 770.
Changing groupname of /opt/oracle/oraInventory to oinstall.
The execution of the script is complete
#
```

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

Display the Oracle Central Inventory Location

Use this procedure to display the location of the Oracle central inventory after STA has been installed. Oracle recommends that you register this location (see "[Register the Oracle Central Inventory Location](#)" on page 3-19 for instructions). Registration creates an Oracle central inventory pointer file, `/etc/orainst.loc`. If the location has not been registered or the pointer file has been deleted, you can use this procedure to display the location.

1. Log in as the system root user or the Oracle install 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. For example:

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

The location is defined by the `inventory_loc` parameter, and the Oracle install group is defined by the `inst_group` parameter.

- 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
#
```

Configuring Library Features for STA

For the libraries to send high-quality SNMP data to STA, selected features must be configured appropriately. These features vary by library model. You should complete the activities in this chapter before continuing to [Chapter 5, "Configuring SNMP on the Libraries"](#).

This chapter includes the following sections:

- [Library Features Affecting STA Data](#)
- [Library User Interfaces](#)
- [Library Feature Configuration Tasks](#)

Library Features Affecting STA Data

- ["ADI Interface for LTO Drives"](#) on page 4-1
- ["Dual TCP/IP and Redundant Electronics \(SL3000 and SL8500 only\)"](#) on page 4-2
- ["Library Complex ID \(SL8500 only\)"](#) on page 4-3
- ["Drive Clean Warning \(SL3000 and SL8500 only\)"](#) on page 4-4
- ["Volume Label Format \(SL500 and SL150 only\)"](#) on page 4-4
- ["SCSI FastLoad Option \(SL500 only\)"](#) on page 4-5
- ["Duplicate Volume Serial Numbers"](#) on page 4-5

ADI Interface for LTO Drives

StorageTek modular libraries support Linear Tape Open (LTO) drives from HP and IBM. 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.

See the *STA Requirements Guide* for details about required drive firmware levels.

Enabling ADI on LTO Drives

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

- **HP LTO-3, LTO-4, LTO-5, and LTO-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-3, LTO-4, LTO-5, and LTO-6:** 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. [Table 4–1](#) provides additional detail.

Note: The Belisarius adapter card provides the interface to the Oracle Key Manager (OKM) tape encryption solution. Both the drive and the Belisarius card firmware must meet the minimum requirements for STA.

Table 4–1 How ADI is Enabled on IBM LTO Drives

IBM LTO Drive	LTO-3	LTO-4	LTO-5, LTO-6
IBM without the Belisarius adapter card	Oracle Support configures the drive hardware for ADI mode.	Oracle Support configures the drive hardware for ADI mode.	NA
IBM with the Belisarius adapter card	NA	Oracle Support configures the drive hardware for ADI mode.	The drive firmware must be configured for ADI mode with Virtual Operator Panel (VOP). Contact Oracle Support for assistance.

Enabling 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 the *STA Requirements Guide* for details about the HBT card.

Dual TCP/IP and Redundant Electronics (SL3000 and SL8500 only)

Redundant Electronics and Dual TCP/IP are optional features for SL3000 and SL8500 libraries.

Dual TCP/IP protects library/host operations from network failures by providing two library TCP/IP ports, typically configured on separate subnets. In the event of network disruptions or failure on one subnet, the library/host connection automatically fails over to the other port.

Redundant Electronics protects against hardware failures on the library controller by providing two separate and fully functional library controller cards—an active and a standby. If the active controller experiences significant errors, library control can be switched to the standby card, with minimal disruption to library and host operations.

See the library *User's Guide* for complete details about these features.

Configuring the STA Connection to Support These Features

Depending on which of these features are activated—Dual TCP/IP, Redundant Electronics, or both—an SL3000 or SL8500 library can have one, two, or four IP addresses. However, 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, but not both.

When you configure the STA connection to the library, you must always specify a primary library IP address. You can optionally specify a secondary IP address, depending on the feature configuration of the library and which feature you want STA to support.

Note: 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 STA is configured to support Dual TCP/IP, STA maintains a connection with the library in the event of a port failover.

If STA is configured to support Redundant Electronics, if a controller card switch occurs, STA maintains a connection with the library through the port specified as the secondary library IP address.

See the library *User's Guide* for more information about these features.

[Table 4-2](#) summarizes the recommended library IP addresses to use when configuring the STA connection to the library.

Table 4-2 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

Additional Considerations for These Features

- To configure STA to support Dual TCP/IP on an SL3000 or SL8500 library, you may need to use policy routing. For more information, consult the SL3000 or SL8500 *Host Connectivity Guide*. If you need assistance with Dual TCP/IP configuration, contact Oracle Support.
- 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 the SNMP Connection to a Library](#)" on page 6-5). 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.

Library Complex ID (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 4–3](#) lists some sample valid SL8500 complex ID assignments.

Table 4–3 Example Complex ID Assignments

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

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.

See "[Ensure the Correct Library Complex ID \(SL8500 only\)](#)" on page 4-9 for instructions.

Drive Clean Warning (SL3000 and SL8500 only)

The drive clean 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.
- 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.

If you have a large number of 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 "[Set the Drive Clean Warning \(optional, SL3000 and SL8500 only\)](#)" on page 4-10 for instructions.

Volume Label Format (SL500 and SL150 only)

Volume serial numbers (volsers) in SNMP data must be formatted properly for STA to process library exchange data correctly. The media volser includes a two-character suffix that indicates the media type. For example, if a cartridge volser is ABC123L4, "L4" indicates the media type is LTO4. For proper STA reporting, the volser suffix must be excluded.

To ensure proper formatting, the following parameters must be set:

- For all SL500 libraries monitored by STA, the label orientation for the host must be set to left6 and STA mode (controlled by the staConfig flag) must be set to on. STA

mode affects only the format of the volser sent to the STA server through SNMP, not the format used on the SL500 library itself.

- For all SL150 libraries monitored by STA, the Volume Label Format must be set to Trim last two characters.

Caution: If these parameters are not set properly, volsers will be formatted incorrectly, causing exchanges processing to be blocked, superfluous attempts to get the latest media data, and irreversible, eight-character volser records to appear on the Media – Overview screen whenever the "Show Removed Media" preference is set.

See ["Set the SL500 Volume Label Format \(SL500 only\)"](#) on page 4-10 and ["Set the SL150 Volume Label Format and Drive Element Addressing Mode \(SL150 only\)"](#) on page 4-11 for instructions.

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.

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.

Library User Interfaces

The SL500, SL3000, and SL8500 libraries have a command line interface (CLI) and a graphical user interface, the StorageTek Library Console (SL Console). The SL150 library uses a browser-based user interface exclusively. You will use these interfaces to perform the procedures in this chapter.

Library CLI Usage Tips

For most CLI commands, the syntax is the same across the SL500, SL3000, and SL8500 library models. For the few commands where the syntax varies by library model, examples are provided. Most CLI examples use an SL500 library. If you are configuring an SL3000 or SL8500 library, 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 should you need 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 library commands are case-sensitive; SL3000 and SL8500 commands are not.
- To avoid entry errors, you can first type a command in a text file, and then copy and paste it into the CLI. For help with CLI commands, type `help snmp`.
- You can reduce keystrokes by using the following CLI features:
 - Press the **Tab** key for automatic command completion.
 - Press the **Up-Arrow** and **Down-Arrow** keys to scroll through your command history. You can modify a previously entered command, and then press **Enter** to execute it.
 - To correct a command before you press **Enter** to execute it, use the **Left-Arrow** and **Right-Arrow** keys to move the cursor to the location of the error, and then type the correction. New characters are inserted at the cursor; to delete characters, use the **Backspace** key.

Library Configuration Script (optional)

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

Note: It is recommended that you review and understand the library configuration steps in this chapter before initiating the script.

To initiate the script, open a terminal session on the STA server 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. See ["Users, Groups, and Locations Used by the STA Installer"](#) on page 3-1 for details.

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
```

Library Feature Configuration Tasks

Use [Table 4-4](#) to determine which tasks apply to the library models at your site. You must perform the applicable tasks on each library you want STA to monitor.

Table 4-4 Tasks to Configure Libraries for STA

Task	SL150	SL500	SL3000	SL8500
"Log In to the Library" on page 4-7	Yes	Yes	Yes	Yes
"Verify the Library Firmware Version" on page 4-7	Yes	Yes	Yes	Yes
"Verify the Drive Controller Card Version (SL3000 and SL8500 only)" on page 4-8	–	–	Yes	Yes

Table 4–4 (Cont.) Tasks to Configure Libraries for STA

Task	SL150	SL500	SL3000	SL8500
"Enable ADI on the Library (all libraries except SL150)" on page 4-9	–	Yes	Yes	Yes
"Ensure the Correct Library Complex ID (SL8500 only)" on page 4-9	–	–	–	Yes
"Set the Drive Clean Warning (optional, SL3000 and SL8500 only)" on page 4-10	–	–	Yes	Yes
"Set the SL500 Volume Label Format (SL500 only)" on page 4-10	–	Yes	–	–
"Set the SL150 Volume Label Format and Drive Element Addressing Mode (SL150 only)" on page 4-11	Yes	–	–	–

Note: For SL500, SL3000, and SL8500 libraries, many tasks allow you to choose which interface to use—CLI or SL Console. For SL150 libraries, you must use the browser-based user interface exclusively.

Log In to the Library

Using the library CLI (all libraries except SL150)

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

Using the SL Console (all libraries except SL150)

1. Start the SL Console application.
2. Click the **About** button to display the current SL Console version and verify that it meets the library firmware minimum requirements.
3. Click **Close** to return to the Login screen.
4. 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.

Using the SL150 user interface

1. Browse to the hostname or IP address of the SL150 library.
2. Log in with your user ID and password. The user ID must have the role of administrator.

Verify the Library Firmware Version

Use this procedure to verify that the library firmware meets or exceeds the minimum requirements stated in the *STA Requirements Guide*. If it does not, submit a service request to Oracle Support to upgrade the firmware.

For SL8500 libraries, Oracle Support must record the network connection settings before performing a firmware upgrade, as these settings may need to be re-entered or updated after the upgrade.

Using the library CLI (all libraries except SL150; not applicable to SL3000 libraries below FRS 4.x.)

1. Execute the following command:

```
SL500> version print
```

```
Library Hardware Information
Library Vendor: STK
...
Firmware Version: xxxx (x.xx.xx)
```

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

Using the SL Console (all libraries except SL150)

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.

The firmware version is displayed under the Code Version section.

Using the SL150 user interface

1. In the navigation tree, select **Firmware**.

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 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. This is mainly a concern for older libraries (shipped before mid-2006), as newer units are shipped with a high-memory card. See the *STA Requirements Guide* for detailed firmware level requirements.

Use this procedure to verify that a high-memory HBT card is installed in the library. If the library does not have a high-memory HBT card, submit a service request to Oracle Support to have one installed.

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 card information.

This procedure is performed using the SL Console.

1. 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.

The screen displays details about the active drive controller (HBT) card.

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, hbfb). Both should indicate True for High Memory HBT.

Note: Both the active and standby HBT cards must be installed and communicating, and both must have high memory.

Enable ADI on the Library (all libraries except SL150)

If your library includes LTO drives, ADI must be enabled on both the drives and the library for STA to receive rich drive data. Use this procedure to ensure that the ADI drive interface is enabled on the library. See ["ADI Interface for LTO Drives"](#) on page 4-1 for details.

This procedure is performed using the library CLI.

For SL3000 or SL8500 Libraries

1. Display the status of the ADI interface.
`drive adiEnable print`
2. If "Attributes Adi Status" is true, you can quit this task. If it is false, proceed to the next step.
3. Enable the ADI interface.
`drive adiEnable on`
4. Reboot the library to activate the change.

For SL500 Libraries

1. Display the status of the ADI interface.
`enableADI print`
2. If "enableADI set to" is on, you can quit this task. If it is set to off, proceed to the next step.
3. Enable the ADI interface.
`enableADI on`
4. Reboot the library to activate the change.

Ensure the Correct Library Complex ID (SL8500 only)

For STA to roll up library complex data correctly, each library complex at your site must have a unique complex ID. Use this procedure to ensure the correct library complex ID for each SL8500 library. See ["Library Complex ID \(SL8500 only\)"](#) on page 4-3 for details.

This procedure is performed using the library CLI.

1. For each SL8500 library that will be monitored by STA, 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
```

Example 4–1 Change standalone SL8500 complex ID

```
SL8500> config complexId set 5
```

```
...
```

```
Complex Id 5
```

```
Success true
```

```
Done
```

```
...
```

```
Note: TCP/IP stack reset may take a few seconds after command completion.
```

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

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

Use this optional procedure to check the current setting of the drive clean warning flag on the library and change it if necessary. See "[Drive Clean Warning \(SL3000 and SL8500 only\)](#)" on page 4-4 for details.

This procedure is performed using the library CLI.

1. 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
```

Set the SL500 Volume Label Format (SL500 only)

Use this procedure to ensure that volume serial numbers (volsers) are formatted correctly in SNMP data sent to STA. See "[Volume Label Format \(SL500 and SL150 only\)](#)" on page 4-4 for details.

This procedure is performed using the SL500 CLI.

Note: Oracle recommends that you quiesce all activity to the library before changing these parameters. Tape applications and/or hosts may require configuration changes after changing these parameters.

1. Display the current setting of 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

2. The host flag must be set to left6. To do so, use the following command:

```
SL500> orientlabel host left6
New settings were accepted...Setting are now in effect.
```

3. Display the setting again to verify it was updated correctly.

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

4. Display the current setting of the staConfig flag.

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

5. The staConfig flag must be set to on. To do so, use the following command:

```
SL500> staConfig on
```

6. Display the setting again to verify it was updated correctly.

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

Set the SL150 Volume Label Format and Drive Element Addressing Mode (SL150 only)

Use this procedure to ensure that volume serial numbers (volsers) are formatted correctly in SNMP data sent to STA.

Also, for SL150 firmware 2.xx and above, use this procedure to set the Drive Element Addressing Mode so that empty drive bays are included in the data sent to STA.

See "[Volume Label Format \(SL500 and SL150 only\)](#)" on page 4-4 for details.

Note: Oracle recommends that you quiesce all activity to the library before changing these parameters. Tape applications and hosts may require configuration changes after changing these parameters.

This procedure is performed using the SL150 browser-based interface.

1. In the navigation tree, select **Configuration**.
2. Select the **Configure** button.
3. In the Configuration Wizard window, select the **Configure Library Settings** check box, and then click **Next**.
4. Set the following parameters accordingly:
 - Drive Element Addressing Mode: **Address All Drive Slots (Recommended)**
 - Library Volume Label Format: **Trim last two characters (Default)**

Note: After changing the Drive Element Addressing Mode, you should wait at least 10 minutes before configuring SNMP in STA.

5. Click **Next**.

6. On the Summary of Configuration Changes screen, select the **Accept all changes** check box, and then click **Apply**.
7. In the Apply Configuration Changes screen, 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**.

Configuring SNMP on the Libraries

For STA to monitor libraries at your site, you must perform some configuration activities on the libraries and some on the STA server. This chapter describes activities performed on the libraries. You should complete the activities in this chapter before continuing to [Chapter 6, "Configuring Library Connections in STA"](#).

This chapter includes the following sections:

- [Understanding Library SNMP Configuration for STA](#)
- [Library SNMP Configuration Tasks](#)

For general information about the SNMP implementation on the StorageTek libraries, see the *StorageTek Modular Libraries SNMP Reference Guide*.

Understanding Library SNMP Configuration for STA

Communication between STA and the libraries it monitors is through the Simple Network Management Protocol (SNMP). 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.

For optimal SNMP security, Oracle recommends using the SNMP v3 protocol for communication between STA and the libraries. The authentication, encryption, and message integrity features in SNMP v3 provide a secure mechanism for sending library data. SNMP v3 is also required for the STA media validation feature. (STA media validation is available for supported libraries only; see the *STA Requirements Guide* for details.)

This chapter describes the recommended SNMP v3 configuration. Depending on your site requirements, however, and if security is not a concern, you may choose to use the less secure SNMP v2c protocol for one or more libraries. See [Appendix F, "Configuring SNMP v2c Mode"](#) for SNMP v2c configuration instructions.

Note: While the SNMP v3 protocol is used for SNMP traps and get functions, the initial communication handshake between a library and STA is always through the SNMP v2c protocol.

Configuring the SNMP v3 Protocol on the Libraries

On each library, you set up SNMP v3 communication between STA and each library by defining the library as an SNMP v3 user and the STA server as an SNMP v3 trap recipient. In addition, you must specify authorization and privacy mechanisms and

passwords. For STA, the authorization method is always SHA (Secure Hash Algorithm), and the privacy method is always DES (Data Encryption Standard).

SNMP v2c Community String

The initial communication handshake between a library and STA is always through the SNMP v2c protocol; therefore, you must define an SNMP v2c community string, even if you are using the recommended SNMP v3 protocol for SNMP communication.

The community string is a password or phrase you assign for the STA community. Following are requirements.

- STA supports only one SNMP v2c community string. You must define the same community string on STA and on all libraries monitored by that STA instance.
- Your libraries may already have one or more SNMP v2c community strings, and you can use one of these for STA; however, Oracle highly recommends defining a new, unique SNMP v2c community string for this purpose.
- Oracle recommends *not* using the values "public" or "private" for the STA community string, as these values are well known and present a security risk. Oracle recommends using values that are not as easily discovered.
- 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).
- The community string can only contain alphanumeric characters (a–z, A–Z, 0–9). Special characters are not allowed.

Unique SNMP v3 User

Following are requirements for the SNMP v3 user.

- STA supports only one SNMP v3 user. You must define the same user on STA and on all libraries monitored by that STA instance.
- Your libraries may already have one or more SNMP v3 users and you can use one of these for STA; however, Oracle highly recommends defining a new, unique SNMP v3 user for this purpose.
- Oracle recommends *not* using the values "public" or "private" for the SNMP v3 username, as these values are well known and present a security risk. Oracle recommends using 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.

To define the SNMP v3 user, you must provide the following values. See [Appendix C](#) for a worksheet you can use to record the values you will use.

SNMP v3 username

The STA server listens for traps sent by this user. It is also the SNMP v3 recipient name used when creating trap recipients. Must be the same on all libraries.

SNMP v3 authorization password

Authorization password you assign to the SNMP v3 user. Must be at least eight characters in length, and cannot contain commas (,), semicolons (;), or equal signs (=).

SNMP v3 privacy encryption password

Privacy password you assign to the SNMP v3 user. Must be at least eight characters in length, and cannot contain commas (,), semicolons (;), or equal signs (=).

SNMP v2c user community

SNMP v2c user community string. Oracle recommends *not* using the values "public" or "private", as these values are well known and present a security risk. See "[SNMP v2c Community String](#)" on page 5-2 for complete requirements.

SNMP v2c trap community

The SNMP v2c trap community string. This field is used only if SNMP v2c is used for communication with the library and is ignored if you are using the recommended SNMP v3 protocol. Oracle recommends *not* using the values "public" or "private", as these values are well known and present a security risk. See "[SNMP v2c Community String](#)" on page 5-2 for complete requirements.

SNMP Engine IDs

Because the SNMP v3 protocol requires each SNMP device to have a globally unique engine ID, the STA server and the libraries each have their own engine IDs. In the case of SL8500 library complexes, each library in the complex also has its own SNMP agent, and therefore its own unique engine ID. The engine ID contains a maximum of 31 hexadecimal characters.

SNMP traps use the *sender's* engine ID; therefore, you must specify the *library* engine ID when you define STA as the SNMP v3 trap recipient.

Library SNMP Configuration Tasks

[Table 5–1](#) summarizes the process for configuring libraries to send proper SNMP data to STA. You must perform the tasks in the order listed, on each library you want STA to monitor.

Table 5–1 Tasks to Configure Libraries for STA

Task	SL150	SL500	SL3000	SL8500
" Retrieve the Library IP Address " on page 5-4	Yes	Yes	Yes	Yes
" Enable SNMP on the Library " on page 5-5	Yes	Yes	Yes	Yes
" Ensure an SNMP v2c User " on page 5-6	Yes	Yes	Yes	Yes
" Create an SNMP v3 User " on page 5-7	Yes	Yes	Yes	Yes
" Retrieve the Library SNMP Engine ID (all libraries except SL150) " on page 5-8	–	Yes	Yes	Yes
" Create the STA SNMP v3 Trap Recipient " on page 5-8	Yes	Yes	Yes	Yes

Note: These procedures assume you are using the recommended SNMP v3 protocol for communication between STA and the libraries. See "[Understanding Library SNMP Configuration for STA](#)" on page 5-1 for details.

Note: For SL500, SL3000, and SL8500 libraries, some tasks allow you to choose which interface to use—CLI or SL Console. For SL150 libraries, you must always use the browser-based user interface.

Retrieve the Library IP Address

Use this procedure to retrieve and record the library IP address, which you will use to configure the connection with the library.

For SL3000 and SL8500 libraries, choose the method to support either Redundant Electronics, Dual TCP/IP, or neither. See "[Dual TCP/IP and Redundant Electronics \(SL3000 and SL8500 only\)](#)" on page 4-2 for details.

This procedure is performed using the SL Console or the SL150 browser-based interface.

SL500 IP Address

1. 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 IP Addresses—Redundant Electronics Support

1. 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 feature 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.
5. Record the IP address of the 2B port.
6. Repeat Step 4 and Step 5 for the alternate (standby) controller card.

SL3000 or SL8500 IP Addresses—Dual TCP/IP Support

1. 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).

SL3000 or SL8500 IP Addresses—Neither Dual TCP/IP Nor Redundant Electronics

1. 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 section. There is no IP address information in the 2A section.
4. Record the IP address as the primary library IP address.

SL150 IP Address

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

Note: The Configure IPxx field value must be **Static**. If it is not, click the **Configure** button, and then select **Configure Network Settings** to specify a static IP address.

Enable SNMP on the Library

Use this procedure to enable SNMP on the library public port.

Using the library CLI

1. Depending on library model, use one of the following commands:
 - For SL3000 and SL8500 libraries, enable SNMP on port 2B. If the library includes the Dual TCP/IP feature, this command also enables SNMP on port 2A.
> `snmp enable port2b`
 - For SL500 libraries, enable SNMP on port 1B.
> `snmp enable port1B`

Using the SL Console (SL500 only)

1. From the **Tools** menu, select **System Detail**.
2. In the navigation tree, select **Library**.
3. Select the **SNMP** tab, then select the **Port Control** tab.
4. Complete the Port Control section as follows:
Port: Select Public (1B).
Command: Select Enable.
5. Click **Apply**.

Using the SL150 user interface

1. In the navigation tree, select **SNMP**.
2. If SNMP shows as disabled, select **Enable SNMP**.
3. In the confirmation window, click **OK**.

Ensure an SNMP v2c User

An SNMP v2c user is required for the initial handshake between the library and the STA server. See "[SNMP v2c Community String](#)" on page 5-2 for complete requirements.

Using the library CLI (all libraries except SL150)

1. Establish a CLI session on the library.
2. 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 stasmp
```

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

```
> snmp listUsers
...
Attributes Community stasmp
Index 1
Version v2c
Object Snmp snmp
...
```

Using the SL Console (SL500 only)

1. Use the SL Console to log in to the library.
2. From the **Tools** menu, select **System Detail**.
3. In the navigation tree, select **Library**.
4. Select the **SNMP** tab and then the **Add Users** tab.
5. Complete the **Add Users** screen as follows:
 - Version: Select v2c.
 - Community: Specify the SNMP v2c user community string (for example, stasmp).
6. Click **Apply**.

Using the SL150 user interface

1. Log in to the library.
2. In the navigation tree, select **Settings**.
3. Select the **SNMP** tab.
4. In the SNMP Users table, select **Add SNMP User**.
5. Complete the Add SNMP User screen as follows:
 - Version: Select v2c.
 - Community Name: Specify the SNMP v2c user community string (for example, stasmp).
6. Click **OK**.

Create an SNMP v3 User

All SNMP traps and MIB (management information base) data are sent to the STA server through the SNMP v3 user. Note the username and passwords you specify, as you will use this information when you define an SNMP v3 trap recipient.

Note the following configuration requirements:

- The authorization method must be SHA (Secure Hash Algorithm), and the privacy method must be DES (Data Encryption Standard).
- All libraries monitored by a single STA instance must have the same SNMP v3 username. You should create a new, unique user for this purpose.
- Authorization and privacy passwords must be at least eight characters in length, and cannot contain commas, semicolons, or equal signs.

Using the library CLI (all libraries except SL150)

1. 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.

Note: For SL3000 and SL8500 libraries, enclose all variables in single quotes ([Example 5-1](#)).

Example 5-1 Create SNMP v3 User on SL3000 or SL8500

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

Example 5-2 Create SNMP v3 User on SL500

```
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
```

Using the SL Console (SL500 libraries only)

1. From the **Tools** menu, select **System Detail**.
2. In the navigation tree, select **Library**.
3. Select the **SNMP** tab, then select the **Add Users** tab.
4. Complete the **Add Users** tab as follows:
 - Version: Select v3.
 - UserName: The name of the SNMP v3 user.
 - Auth: Select SHA.

- AuthPass: Specify an authorization password.
 - Priv: Select DES.
 - PrivPass: Specify a privacy password.
5. Click **Apply**.

Using the SL150 user interface

1. In the navigation tree, select **SNMP**.
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.
4. Click **OK**.

Retrieve the Library SNMP Engine ID (all libraries except SL150)

Use this procedure to display the library's SNMP engine ID (for example, 0x81031f88804b7e542f49701753).

This procedure is performed using the library CLI.

1. Depending on the library model, use one of the following commands:
 - For SL3000 and SL8500 libraries:

```
> snmp engineId print
```
 - For SL500 libraries:

```
> snmp engineId
```
2. Save the engine ID to a text file for use in the remaining SNMP configuration tasks.

Create the STA SNMP v3 Trap Recipient

Use this procedure to define the STA server as an authorized recipient of SNMP traps, and to 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) are new for 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.

Using the library CLI (all libraries except SL150)

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 ["Create an SNMP v3 User"](#) on page 5-7.
- *auth_password* and *priv_password* are the authorization and privacy passwords you created in ["Create an SNMP v3 User"](#) on page 5-7.
- *library_engineID* is the library engine ID you displayed in ["Retrieve the Library SNMP Engine ID \(all libraries except SL150\)"](#) on page 5-8, including the 0x prefix.

Note: For SL3000 and SL8500 libraries, enclose *recipient_name*, *auth_password*, and *priv_password* in single quotes ([Example 5-3](#)).

Example 5-3 Create SNMP v3 Trap Recipient on SL3000 or SL8500

```
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
0x00abcdef00000000000000000000
```

Example 5-4 Create SNMP v3 Trap Recipient on SL500

```
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
0x00abcdef00000000000000000000
```

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

```
> snmp listTrapRecipients
```

Using the SL Console (SL500 libraries only)

1. From the **Tools** menu, select **System Detail**.
2. In the navigation tree, select **Library**.
3. Select the **SNMP** tab, then select the **Add Trap Recipients** tab.
4. Complete the Trap Recipients screen fields as follows:
 - **Host:** The IP address of the STA server.
 - **TrapLevel**—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.
 - **TrapUserName:** SNMP username you created in ["Create an SNMP v3 User"](#) on page 5-7.
 - **Auth**—Select SHA.
 - **AuthPass**—Authorization password you created in ["Create an SNMP v3 User"](#) on page 5-7.

- Priv—Select DES.
 - PrivPass—Privacy password you created in ["Create an SNMP v3 User"](#) on page 5-7.
 - EngineID—Library engine ID you displayed in ["Retrieve the Library SNMP Engine ID \(all libraries except SL150\)"](#) on page 5-8. Do not enter the 0x prefix.
5. Click **Apply**.

Using the SL150 user interface

1. In the navigation tree, select **SNMP**.
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 in ["Create an SNMP v3 User"](#) on page 5-7.
 - Authentication Protocol—Select SHA.
 - Authentication Passphrase—Authorization password you created in ["Create an SNMP v3 User"](#) on page 5-7.
 - Privacy Protocol—Select DES.
 - Privacy Passphrase—Privacy password you created in ["Create an SNMP v3 User"](#) on page 5-7.
 - Engine ID—This field will be supplied automatically. Do not modify the value.
4. Click **OK**.

Configuring Library Connections in STA

For STA to monitor libraries at your site, you must perform some configuration activities on the libraries and some on the STA server. This chapter describes activities performed on the STA server.

This chapter includes the following section:

- [STA Configuration Tasks](#)

STA Configuration Tasks

You must complete the procedures in the order listed. Once you have completed this process, STA can begin monitoring the libraries and performing analytics.

- ["Log In to STA"](#) on page 6-1
- ["Verify SNMP Communication With a Library"](#) on page 6-2
- ["Configure SNMP Client Settings for STA"](#) on page 6-4
- ["Configure the SNMP Connection to a Library"](#) on page 6-5
- ["Test a Library SNMP Connection"](#) on page 6-7
- ["Perform a Manual Data Collection"](#) on page 6-9

Log In to STA

Use this procedure to log in to STA to perform the other procedures in this section. See the *STA User's Guide* for full instructions.

Note: The first login to STA after installation 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.

1. Start a supported Web browser on your computer and enter the URL of the STA application.

`http(s)://STA_host_name:port_number/STA/`

Where:

- *host_name* is the hostname of the STA server.
- *port_number* 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. At the Login screen, enter the STA administrator username and password.

Verify SNMP Communication With a Library

Use this procedure to confirm a good SNMP connection between the STA server and a library.

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.

Perform this procedure for each monitored library. For SL3000 or SL8500 libraries with either Redundant Electronics or Dual TCP/IP, perform this procedure twice for the library: once for the primary library IP address and once for the secondary IP address.

Note: This procedure is performed from the system command line on the STA server.

1. Open a terminal window on the STA server, and log in as the system root user.
2. Test the SNMP v3 connection. The values you specify must match the corresponding ones on the library.

```
# snmpget -v3 -u SNMP_user -a SHA -A auth_pwd -x DES -X priv_pwd -l authPriv
library_IP_addr 1.3.6.1.4.1.1211.1.15.3.1.0
```

Where:

- v3 indicates SNMP v3
- *SNMP_user* is the SNMP v3 username.
- SHA indicates the authentication protocol.
- *auth_pwd* is the authorization password.
- DES indicates the privacy protocol.
- *priv_pwd* is the privacy password.
- *authPriv* indicates that privacy is performed on the command.
- *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.

Example 6-1 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"
```

Example 6-2 Failed snmpget Command—Network Timeout

```
# 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.
```

Example 6-3 Failed snmpget Command—Invalid Password

```
# 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)
```

3. Test the SNMP v2c connection.

```
# snmpget -v2c -c stasnmp -l authPriv library_IP_addr
```

Where:

- -v2c indicates SNMP v2c
 - -c stasnmp indicates the SNMP v2c community string.
 - -l authPriv indicates that privacy is performed on the command.
 - *library_IP_addr* is the IP address of the public port on the library.
4. If both SNMP connection tests are successful, you can quit this procedure. If either test fails, proceed to the next step to troubleshoot suspected network issues, as necessary.
5. Confirm packet routing from the STA server to the library.

```
# traceroute -I library_IP_addr
```

Where:

- -I (uppercase "I") indicates to use Internet Control Message Protocol (ICMP) echo request packets instead of User Datagram Protocol (UDP) datagrams.
- *library_IP_addr* is the IP address of the public port on the library.

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.

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

```
# tcpdump -v host library_IP_addr > /var/tmp/file_name &
```

Where:

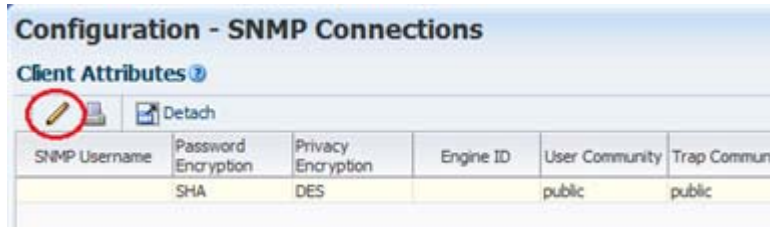
- -v indicates verbose output.
- host indicates to collect packets to or from the indicated host only (in this case, the library).
- *library_IP_addr* is the IP address of the public port on the library.
- *file_name* is the name of the file to which to save the output.

Configure SNMP Client Settings for STA

Use this procedure to add or modify SNMP client settings for STA. These settings configure STA to receive SNMP data from one or more libraries.

There is just one SNMP client entry for each STA instance at your site.

1. From the **Setup & Administration** tab, select **Configuration**, then select **SNMP Connections**.
2. Proceed as follows:
 - To configure the client settings for the first time, select the empty table row in the Client Attributes table, then click **Edit**.



- To modify existing client settings, select the entry in the Client Attributes table, then click **Edit**.



The Define SNMP Client Settings dialog box appears. If this is a new configuration, the fields are blank.

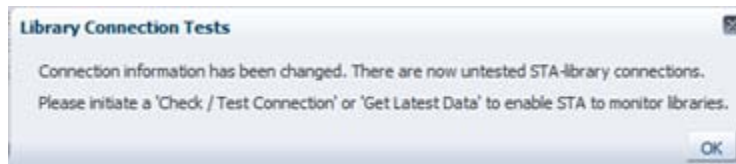
3. Complete the dialog box as follows. The values you specify must match the corresponding ones on the libraries.

Note: 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.

- 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**.

The configuration record is updated, and a message box is displayed, indicating you should perform a library connection test to establish or re-establish the SNMP communication handshake with the libraries.



5. Click **OK** to dismiss the message.

Configure the SNMP Connection to a Library

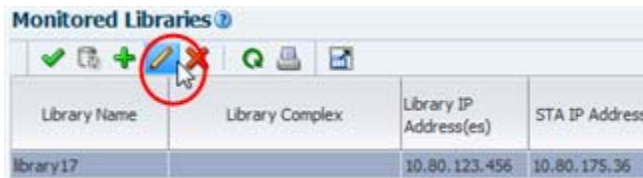
Use this procedure to configure an SNMP connection to each library you want STA to monitor, or to modify an existing connection. For existing connections, you *must* perform this procedure if there are changes to any of the SNMP configuration settings on a monitored library, such as a change to the library IP address.

Note: 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. From the **Setup & Administration** tab, select **Configuration**, then select **SNMP Connections**.
2. Proceed as follows:
 - To configure a connection to a library for the first time, click **Add** in the Monitored Libraries toolbar.



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



The Define Library Connection Details dialog box appears. If this is a new library connection, the fields are blank.

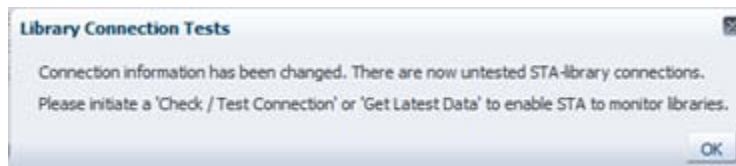
3. Complete the dialog box as follows. The values you specify must match the corresponding ones on the library.
 - Library Name—Type a name to identify the library throughout the STA user interface screens (for example, the library host name).
 - Library Primary IP Address—Type the IP address of the primary public port on the library. You cannot specify the IP address of another monitored library.
 - Library Secondary IP Address—Applies only to SL3000 and SL8500 libraries using Dual TCP/IP or Redundant Electronics. Specify the IP address of the secondary public port on the library. You cannot specify the IP address of another monitored library. Leave the field blank for all other libraries, including all SL500 and SL150 libraries.
 - 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.

4. Click **Save**.

The configuration record is updated, and a message box is displayed, indicating you should perform a library connection test to establish or re-establish the SNMP communication handshake with the libraries.



5. Click **OK** to dismiss the message.

If you have modified an existing library connection, the Library Engine ID field in the Monitored Libraries table is cleared, indicating the SNMP connection has been dropped.

Test a Library SNMP Connection

Use this procedure to test the SNMP connection between STA and a library and establish or re-establish the communication handshake. To avoid dropped connections and lost SNMP traps, you should perform this procedure for each monitored library whenever you add or change SNMP configuration settings for the library or the STA client.

You can test only one library connection at a time.

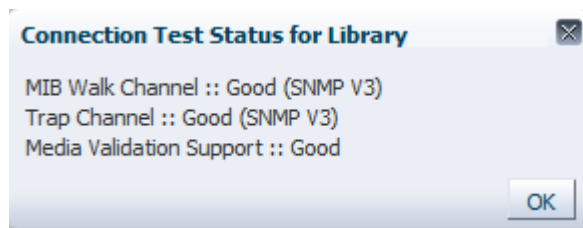
Note: Because a connection test can cause a momentary loss of incoming SNMP packets, you should perform this procedure only when necessary.

Note: Before performing this procedure, you may want to verify that the library is operational.

1. From the **Setup & Administration** tab, select **Configuration**, then select **SNMP Connections**.
2. In the Monitored Libraries table, select a library, then click **Check / Test Connection**.

Library Name	Library Complex	Library IP Address(es)	STA IP Address	Library Engine ID	Recent SNMP Trap Communication Status	Automated Daily Data Refresh Time	Library Time Zone	Last Suc Connect
Crimson11	SL3000_571000200060	10.80.104.51	10.80.175.36	0x80001f88043130303030303030303030	GOOD	00:00:00	UTC	2014-05
Crimson14	SL3000_571000000001	10.80.104.54	10.80.175.36	0x80001f88043130303030303030303030	NO RECENT TRAPS	00:00:00	UTC	2014-05
Crimson19	SL3000_571000200007	10.80.87.13	10.80.175.36	0x80001f88043537313030303030303030	GOOD	00:00:00	UTC	2014-05
elb18	SL8500_2	10.80.104.98	10.80.175.36	0x80001f88043630303030303030303030	GOOD	00:15:00	US/Mountain	2014-05

The Connection Test Status message box appears, displaying results for the MIB Walk Channel, Trap Channel, and Media Validation Support tests.



3. Click **OK** to dismiss the message box.

The Monitored Libraries table is updated with the results of the test.

Library Name	Library Complex	Library IP Address(es)	STA IP Address	Library Engine ID	Recent SNMP Trap Communication Status	Automated Daily Data Refresh Time	Library Time Zone	Last Suc Connect
Crimson14	SL3000_571000000001	10.80.104.54	10.80.175.36	0x80001f88043130303030303030303030	GOOD	00:00:00	UTC	2014-05
Crimson19	SL3000_571000200007	10.80.87.13	10.80.175.36	0x80001f88043537313030303030303030	GOOD	00:00:00	UTC	2014-05
elb18	SL8500_2	10.80.104.98	10.80.175.36	0x80001f88043630303030303030303030	GOOD	00:15:00	US/Mountain	2014-05

- If the Library Complex field is blank, it will be supplied after you perform a manual data collection.
 - Library Engine ID indicates the unique SNMP engine ID for the library.
 - Last Connection Attempt indicates the date and time when the connection test was initiated.
 - Last Successful Connection indicates the date and time when the test was completed, if successful.
 - Last Connection Status indicates the results of the test. If the test fails, STA provides information in the Last Connection Failure Detail field. (You may need to extend the column width to see the entire value.)
4. If the test fails, repeat this procedure as follows:
 - 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 test fails for any other reason, edit the connection details for the library and clear the Library Engine ID field before repeating this procedure. See ["Configure the SNMP Connection to a Library"](#) on page 6-5 for instructions.

Perform a Manual Data Collection

Use this procedure to initiate a manual data collection for a library and get the latest library configuration data. If this procedure is completed successfully, STA begins monitoring the library and performing analytics on the data.

Although STA performs a data collection automatically every 24 hours at the scheduled time, you must perform a manual data collection for each monitored library whenever you add or change SNMP configuration settings for the library or the STA client.

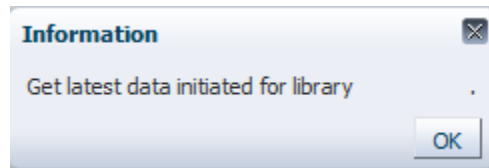
Data collections may take several minutes to an hour, depending on library size.

Note: You can run multiple 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. From the **Setup & Administration** tab, select **Configuration**, then select **SNMP Connections**.
2. Select a library in the Monitored Libraries table, and then click **Get latest data**. You can select only one library at a time.

Library Name	Library Complex	Library IP Address(es)	STA IP Address	Library Engine ID
SL150_abc		192.0.2.20	192.0.2.21	0x80001f8804303

A confirmation message box appears.



3. Click **OK** to dismiss the message box.

The data collection proceeds, and the Monitored Libraries table is updated with the results.

- Library Complex indicates the library complex ID.
- Library Engine ID indicates the unique SNMP engine ID for the library.
- Last Connection Attempt indicates the date and time when the data collection was initiated.
- Last Successful Connection indicates the date and time when the data collection was completed, if successful.
- Last Connection Status is updated as follows:
 - IN PROGRESS: The data collection process is underway.
 - SUCCESS: The data collection was successful. STA starts receiving exchange data from the library.

- **FAILED:** The data collection was not successful. If possible, STA provides information in the Last Connection Failure Detail field. (You may need to extend the column width to see the entire value.)

Note: The status is updated every four minutes, and the default screen refresh interval is 480 seconds. However, you can click the **Refresh Table** button to force a refresh of the table at any time.



-
- Recent SNMP Trap Communication Status may intermittently indicate MISSED HEARTBEAT. This is normal.

Configuring STA Services

Use these procedures to configure the STA Backup service and STA Resource Monitor service utilities.

This chapter includes the following sections:

- [STA Services Overview](#)
- [STA Services Configuration Tasks](#)

STA Services Overview

- STA database backup service—You configure the STA backup service with its administration utility, `staservadm`. To display a complete list of command options for the utility, type `staservadm -h`. See the *STA Administration Guide* for details.
- STA resource monitor service—You configure the STA resource monitor service with its administration utility, `staresmonadm`. To display a complete list of command options for the utility, type `staresmonadm -h` at the command line. See the *STA Administration Guide* for details.

These service utilities are located in the `/Oracle_storage_home/StorageTek_Tape_Analytics/common/bin` directory. See "Users, Groups, and Locations Used by the STA Installer" on page 3-1 for details about the Oracle storage home.

STA Services Configuration Tasks

General Tasks

- ["Update the System Path \(optional\)"](#) on page 7-2
- ["Restart the STA Services Daemon \(optional\)"](#) on page 7-2
- ["Verify Library Connectivity"](#) on page 7-2

STA Database Backup Configuration Tasks

- ["Review the STA Database Backup Utility Preferences"](#) on page 7-2
- ["Configure the Remote Database Backup Server"](#) on page 7-3
- ["Configure the STA Database Backup Service"](#) on page 7-4

STA Resource Monitor Configuration Tasks

- ["Review the STA Resource Monitor Utility Preferences"](#) on page 7-5
- ["Configure the STA Resource Monitor"](#) on page 7-7

Update the System Path (optional)

Use this procedure to ensure that the STA bin directory is included in the PATH variable for the system root user. The bin directory includes the STA service utilities, `staservadm` and `staresmonadm`.

1. Open a terminal session on the current STA server, and log in as the system root user.
2. Use a text editor to open the root user profile. For example:

```
# vi /root/.bash_profile
```

3. 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.

4. Save and exit the file.
5. Log out and log back in as the system root user.
6. Confirm that the PATH variable has been updated correctly.

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

Restart the STA Services Daemon (optional)

Use this procedure to restart the STA Services daemon, `staservd`.

This procedure is useful if you changed the configuration settings of the STA Backup or STA Resource Monitor services and you want the new settings to take effect immediately. If you do not use this procedure, the new settings will take effect as soon as the service wakes up from its sleep interval and processes them.

1. Stop the STA Services daemon.
2. Start the STA Services daemon.
3. Display the status of the daemon to confirm that it is running.

```
# STA stop staservd
```

```
# STA start staservd
```

```
# STA status staservd
```

Verify Library Connectivity

When you have finished configuring the services, confirm that all configured libraries have completed their "Get latest data" requests (Last Connection Status should indicate SUCCESS, and STA should be receiving exchange data from the libraries). See the *STA User's Guide* for details.

Review the STA Database Backup Utility Preferences

Review [Table 7-1](#) for descriptions of the available preference settings and to define your settings.

Table 7-1 STA Backup Service Administration Utility (staservadm) Attributes

Option	Attribute	Description	Default Value	Your Value
-S, --scp -F, --ftp	File transfer type	Method of file transfer used to copy the backup files from the STA server to the backup host. Options are SCP (recommended) or FTP.	SCP	
-T, --time	Full backup dump time	Time of day STA performs a full database backup dump. The dump is performed automatically every 24 hours at approximately this time. The actual time is sometime within "sleep interval" seconds after this time. Format is hh:mm, using 24-hour time.	00:00	
-i, --int	Sleep interval	Number of seconds the STA Services daemon waits before checking for new incremental backup files.	300	
-s, --server	Backup host name	IPv4 or IPv6 address or fully qualified DNS host name of the server host to which the STA server copies its backup files.	NA	
-u, --usr	Backup user ID	System user ID authorized to perform SCP file transfers to the backup host.	NA	
-p, --pwd	Backup password	Password assigned to the backup user.	NA	
-d, --dir	Backup directory	Directory on the backup host where the backup files will be copied.	NA	
-U, --dbusr	Database username	Database username authorized to perform a mysqldump command. You should specify the STA Database DBA Account username.	NA	
-P, --dbpwd	Database password	Password of the database username.	NA	

Configure the Remote Database Backup Server

Use this procedure to configure a remote backup server (or equivalent) to receive the compressed backup files generated by the STA database backup service. Oracle recommends that you configure a remote backup server.

The required space is variable—the size should be a multiple of the size used for the STA database local backup, depending on the number of copies to be retained. Backup server storage should be mirrored or striped.

Note: This procedure is performed on the remote backup server.

1. Log in as the system root user.
2. Create a new group for the STA Backup user. For example:

```
# groupadd -g 54321 stabckgr
```

In this example, the group ID is "stabckgr", and the -g option is used to specify a numerical GID.

3. Create the STA Backup user. For example:

```
# adduser stabck -c "STA database backup user" -m -d /home/stabck -g stabckgr -s /bin/bash -u 98765
```

In this example, the user ID is "stabck", and the following options are used:

- -c – Comment.

- -m – Create a home directory for the user.
 - -d – Absolute path of the home directory.
 - -g – Assign the user to the specified group.
 - -s – Assign the specified login shell to the user.
 - -u – Assign the specified numerical UID to the user.
4. Assign a password to the STA Backup user. For example:

```
# passwd stabck
Changing password for user stabck.
New UNIX password: bckpwd1
Retype new UNIX password: bckpwd1
passwd: all authentication tokens updated successfully.
```

5. Create the directory where the STA backups will be copied. For example:

```
# cd /home/stabck
# pwd
/home/stabck
# mkdir -p STAbackups
# ls
STAbackups
```

In this example, the "STAbackups" directory is created in the STA Backup user's home directory, and the -p option is used to make parent directories as needed.

6. Display the user attributes to confirm that all information has been entered correctly. For example:

```
# cat /etc/passwd |grep sta
stabck:x:98765:54321:STA database backup user:/home/stabck:/bin/bash
```

7. Assign exclusive ownership and access rights for the directory to the STA Backups user and group. For example:

```
# chown -R stabck:stabckgr STAbackups
# chmod -R 700 STAbackups
# chmod 755 /home/stabck
```

In this example, the -R option is used to recursively assign the attributes to the directory and its files.

8. List the directory to confirm that all information has been entered correctly. For example:

```
# ls -la |grep STA
drw----- 2 stabck stabckgr 4096 Oct 19 14:20 STAbackups
```

Configure the STA Database Backup Service

Use this procedure to configure the STA database backup service. You can designate a directory where the backup files will be copied. Oracle recommends that this directory be located on a remote backup server.

Your configuration settings take effect as soon as the service wakes from its current sleep interval and processes new settings or you manually restart the STA Services daemon ("[Restart the STA Services Daemon \(optional\)](#)" on page 7-2).

1. On the STA server, log in as the system root user.
2. Display the current STA Backup Service settings using the staservadm -Q command.

This example shows that the service is not yet configured and is therefore not performing backups.

```
# ./staservadm -Q
Contacting daemon...connected.
Querying Preferences.
Current STA Backup Service Settings:
Configured          [no]
File Transfer       -S [SCP]
Full Backup         -T [00:00]
Sleep Interval      -i [300 sec]
Backup Hostname     -s []
Backup Username     -u []
Backup Password     -p []
Backup Directory    -d []
Database Username   -U []
Database Password   -P []
```

- Using [Table 7-1](#) as a reference, set the attribute values with the `staservadm` command.

You can submit the attributes in separate commands or combine them into one. For example:

```
# ./staservadm -S -T 11:00 -i 350 -s stabaksvr -u stabck -p bckpwd1 -d
/home/stabck/STAbackups -U sta_dba -P password1
```

The utility sets each value included in your command and then displays all current settings. For example:

```
Contacting daemon...connected.
Setting File Transfer Type... SCP
Setting Sleep Interval..... 350
Setting Backup Hostname..... stabaksvr
Setting Backup Username..... stabck
Setting Backup Password..... *****
Setting Backup Directory..... /home/stabck/STAbackups
Setting Full Backup Time.... 11:00
Setting Database Username... sta_dba
Setting Database Password... *****
Done.
Current STA Backup Service Settings:
Configured          [yes]
File Transfer       -S [SCP]
Full Backup         -T [11:00]
Sleep Interval      -i [350 sec]
Backup Hostname     -s [stabaksvr]
Backup Username     -u [stabck]
Backup Password     -p [*****]
Backup Directory    -d [/home/stabck/STAbackups]
Database Username   -U [sta_dba]
Database Password   -P [*****]
```

- Review the command output to verify that the values have been set correctly.

Review the STA Resource Monitor Utility Preferences

Review the option descriptions in [Table 7-2](#) and define your settings. A default value of "-1" indicates the attribute has not been configured.

Table 7-2 STA Resource Monitor (staresmonadm) Attributes

Option	Attribute	Description	Default Value	Your Value
-T, --time	Daily report time	Time of day STA sends a standard daily report. The report is sent automatically every 24 hours at approximately this time. The actual time is sometime within "sleep interval" seconds after this time. Format is hh:mm, using 24-hour time.	00:00	
-i, --interval	Sleep interval	Number of seconds the STA Resource Monitor waits between scans.	300	
-n, --nag	Nag mode	Indicates how frequently STA alerts if any high watermarks are reached. If set to "on", STA sends alert emails every time the system is scanned. If set to "off", alerts are simply noted in the standard daily report.	Off	
-U, --dbusr	Database username	Database username authorized to perform queries against the "information_schema" tables and the MySQL server internal system global variables. You should specify either the STA Database DBA Account username or STA Database Root Account username (root).	NA	
-P, --dbpwd	Database password	The password assigned to the database username.	NA	
-t, --tblsphwm	Database tablespace HWM	High watermark for the database tablespace, entered as a percentage of the maximum available.	-1	
-b, --backvolhwm	Local backup HWM	High watermark for the STA database local backups volume (for example, /dbbackup), entered as a percentage of the maximum possible.	-1	
-d, --dbvolhwm	Database disk volume HWM	High watermark for the STA database volume (for example, /dbdata), entered as a percentage of the maximum available.	-1	
-l, --logvolhwm	Logging disk volume HWM	High watermark for the STA database logs (default is /var/log/tbi), entered as a percentage of the maximum available.	-1	
-z, --rootvolhwm	Root volume HWM	High watermark for the root volume (/), entered as a percentage of the maximum available.	-1	
-x, --tmpvolhwm	Tmp volume HWM	High watermark for the temporary directory volume (default is /tmp), entered as a percentage of the maximum available.	-1	
-m, --memhwm	Physical memory (RAM) HWM	High watermark for the total system memory (except virtual memory), entered as a percentage of the maximum available.	-1	
-f, --from	Email from	Name or email address that appears in the "From" field of the standard daily report email.	StaResMon@localhost	
-r, --recips	Email recipients	Recipient email addresses, entered as a colon-delimited list.	NA	
-s, --subject	Email subject	Entry that appears in the "Subject" field of the standard daily report email, up to 128 characters. Use quotes if it contains spaces. A timestamp in yyyy-mm-dd hh:mm:ss form will be appended to your entry when the email is sent.	STA Resource Monitor Report	
-o, --outfile	Output data file	Absolute path of the comma-separated (CSV) output data file.	/STA_logs/db/staresmon.csv For example: /var/log/tbi/db/staresmon.csv	

Configure the STA Resource Monitor

Use this procedure to configure the STA Resource Monitor service. Your configuration settings take effect as soon as the service wakes from its current sleep interval and processes new settings or you manually restart the STA Services daemon ("[Restart the STA Services Daemon \(optional\)](#)" on page 7-2).

Note: Oracle recommends that usage for any partition should never exceed 80 percent.

1. On the STA server, log in as the system root user.
2. Display the current STA Resource Monitor settings using the `staresmonadm -Q` command.

This example shows the service is not yet configured and is therefore not performing scans.

```
# ./staresmonadm -Q
Contacting daemon...connected.
Querying Preferences.
Current STA Resource Monitor Service Settings:
Configured                               [no]
Send Reports                             -T [00:00]
Sleep Interval                            -i [300 sec]
Alert Nagging                             -n [off]
DB Username                               -U []
DB Password                               -P []
DB Tablespace hwm                         -t [-1%]
DB Backup hwm (/dbbackup)                 -b [-1%]
DB Data hwm (/dbdata)                     -d [-1%]
Log Volume hwm (/var/log/tbi)              -l [-1%]
Root Volume hwm (/)                       -z [-1%]
Tmp Volume hwm (/tmp)                     -x [-1%]
System Memory hwm                         -m [-1%]
Email 'From:'                             -f [StaResMon@localhost]
Email 'To:'                               -r []
Email 'Subject:'                          -s [STA Resource Monitor Report]
Output File                               -o [/var/log/tbi/db/staresmon.csv]
```

3. Using [Table 7-2](#) as a reference, set the attribute values with the `staresmonadm` command.

You can submit the attributes in separate commands or combine them into one. For example:

```
# ./staresmonadm -T 13:00 -i 600 -n on -U sta_dba -P password1 -t 65 -b 65 -d
65 -l 65 -z 70 -x 80 -m 75 -r john.doe@company.com
```

The utility sets each value included in your command and then displays all current settings. For example:

```
Contacting daemon...connected.
Setting DB Tablespace HWM..... 65
Setting DB Disk Volume HWM.... 65
Setting Logging Volume HWM.... 65
Setting Backup Volume HWM..... 65
Setting Root Volume HWM..... 70
Setting Temp Volume HWM..... 80
Setting System Memory HWM..... 75
```

```

Setting 'To:' addresses..... john.doe@company.com
Setting Send Time..... 13:00
Setting Sleep Interval..... 600
Setting Alert Nag Mode..... ON
Setting DB Username..... sta_dba
Setting DB Password..... *****
Done.
Current STA Resource Monitor Service Settings:
Configured                [yes]
Send Reports               -T [13:00]
Sleep Interval            -i [600 sec]
Alert Nagging             -n [on]
DB Username               -U [sta_dba]
DB Password               -P [*****]
DB Tablespace hwm        -t [65%]
DB Backup hwm (/dbbackup) -b [65%]
DB Data hwm (/dbdata)    -d [65%]
Log Volume hwm (/var/log/tbi) -l [65%]
Root Volume hwm (/)      -z [70%]
Tmp Volume hwm (/tmp)    -x [80%]
System Memory hwm        -m [75%]
Email 'From:'            -f [StaResMon@localhost]
Email 'To:'              -r [john.doe@company.com]
Email 'Subject:'         -s [STA Resource Monitor Report]
Output File              -o [/var/log/tbi/db/staresmon.csv]

```

4. Review the command output to verify that the values have been set correctly.

Upgrading to STA 2.2.x

This chapter provides instructions for upgrading any previously released version of STA to STA 2.2.0 and subsequent STA 2.2.x versions. It includes the following sections:

- [Upgrade Paths](#)
- [Upgrade Process Overview](#)
- [Environment Changes](#)
- [Preparation Tasks for All Upgrades](#)
- [Post-installation Upgrade Tasks](#)
- [Post-upgrade Tasks for All Upgrades](#)

If you are installing STA for the first time, you should perform a new base installation; see [Chapter 3, "Installing STA"](#) for instructions.

[Appendix C](#) includes worksheets you can use to organize your upgrade activities and record your settings.

Note: The upgrade to STA 2.2.x is a *post-installation* upgrade, which is a manual process. See "[Understanding Automatic and Post-installation Upgrades](#)" on page 8-2 for definitions of the upgrade types.

Upgrade Paths

You can upgrade to STA 2.2.x from any of the following released STA versions. See "[Verify Upgrade Prerequisites](#)" on page 8-7 to determine your current STA version.

- STA 2.1.x:
 - STA 2.1.64.124
- STA 2.0.x:
 - STA 2.0.0.83
 - STA 2.0.1.4
- STA 1.0.x:
 - STA 1.0.0.99
 - STA 1.0.1.133
 - STA 1.0.2.24

Note: If you are upgrading from STA 1.0.x, you must also install a new version of Linux before installing STA 2.2.x. See the *STA Requirements Guide* for details.

Upgrade Process Overview

During an upgrade, your existing STA data is transformed from the current STA version to the new. Your existing STA database is not valid with the new version of STA until these transformations are done. After the upgrade, STA processes new data according to the new STA schema and analytic rules, and historical data is not reprocessed.

Preparing for the Upgrade

Before beginning the upgrade, read all instructions in this chapter, and be sure to allocate sufficient time for the entire process. 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 itself in as little time as possible.

While you are performing the upgrade process, STA does not receive exchange information from the monitored libraries. Additionally, the new version of STA does not begin receiving information from the libraries until after you have completed all steps in the upgrade and tested the SNMP connection to each monitored library.

Understanding Automatic and Post-installation Upgrades

Depending on the new version of STA and your upgrade path, the upgrade may be either *automatic* or *post-installation*, as follows:

Automatic upgrades

In an automatic upgrade, the STA installer takes a snapshot of your current data, installs the new version of STA, and then upgrades your data to the new version. All these activities are handled automatically by the STA upgrade installer.

Automatic upgrades are possible when the underlying operating system, database, and installation framework are consistent from one version of STA to the next. For example, the upgrades from STA 2.0 to STA 2.0.1 and from STA 1.0 to STA 1.0.2 are automatic upgrade.

Post-installation upgrades

In a post-installation upgrade, you must take a snapshot of your existing data, then deinstall the current version of STA and install the new one, and then run a supplied script to upgrade your data to the new version. You must perform these activities manually and in the proper sequence. Depending on the new STA version, you may also need to install a new version of Linux on the STA server before installing STA.

Post-installation upgrades are necessary in the following situations:

- The new version of STA requires a new version of Linux. For example, STA 1.0.x requires Linux 5, while STA 2.0 and subsequent versions require Linux 6; therefore, to upgrade to STA 2.0 or higher from STA 1.0.x, a new version of Linux must be installed, which requires a post-installation upgrade.
- The STA installation framework has changed significantly. For example, the installer for STA 2.1.0 and subsequent versions use the Oracle Universal Installer

framework; therefore, upgrading to STA 2.1.x or STA 2.2.x from any previous version of STA requires a post-installation upgrade.

Post-installation Upgrades: Choosing Whether to Use One Server or Two

For post-installation upgrades, you can choose to use either one server or two, depending on your goals and available resources. Automatic upgrades are by nature always done on one server.

The upgrade tasks are largely the same for the two methods, but the tasks are performed in different orders. The two methods are discussed in the following sections:

- "Single-server Upgrade Method" on page 8-3
- "Two-server Upgrade Method" on page 8-4

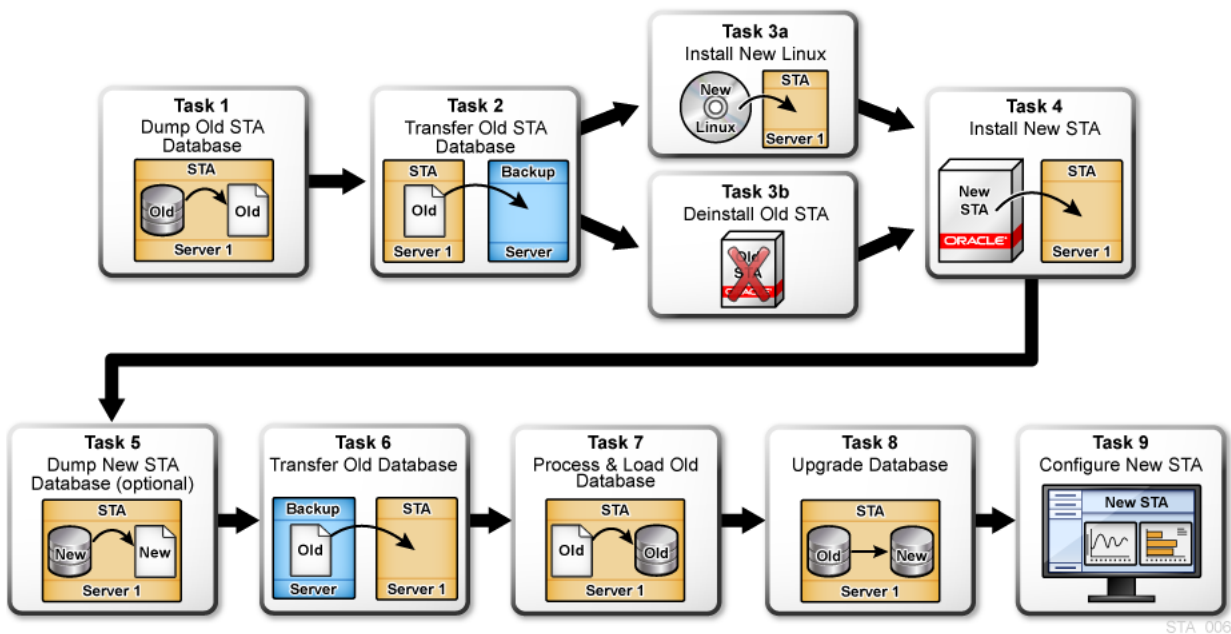
Single-server Upgrade Method

Using the single-server method, you must deinstall STA before you install the new version and upgrade the database on the same server. STA is not monitoring libraries while you perform this process.

This method offers the advantage of not requiring an additional dedicated server for the upgrade. If you are upgrading from STA 2.0 or higher, you do not need to install a new version of Linux, so this method may be sufficient for your needs.

[Figure 8–1](#) illustrates the single-server method. You perform Task 1 through Task 9 in sequential order. In summary:

- Dump the current database and transfer it to a backup server for safekeeping (Task 1 and Task 2).
- Depending on your current version of STA, either install Linux 6.x (Task 3a) or Deinstall STA 2.0.x (Task 3b).
- Install STA 2.2.x, and as a precaution, dump the new database (Task 4 and Task 5).
- Transfer the dump of the old database from the backup server, and then load and upgrade it to the new STA version (Task 6 through Task 8).
- Reestablish connections to the monitored libraries and perform necessary manual configuration tasks (Task 9). Because the old version of STA must be deinstalled before you install STA 2.2.x, you must reenter some user configuration data manually.

Figure 8–1 Single-server Upgrade Task Overview

Two-server Upgrade Method

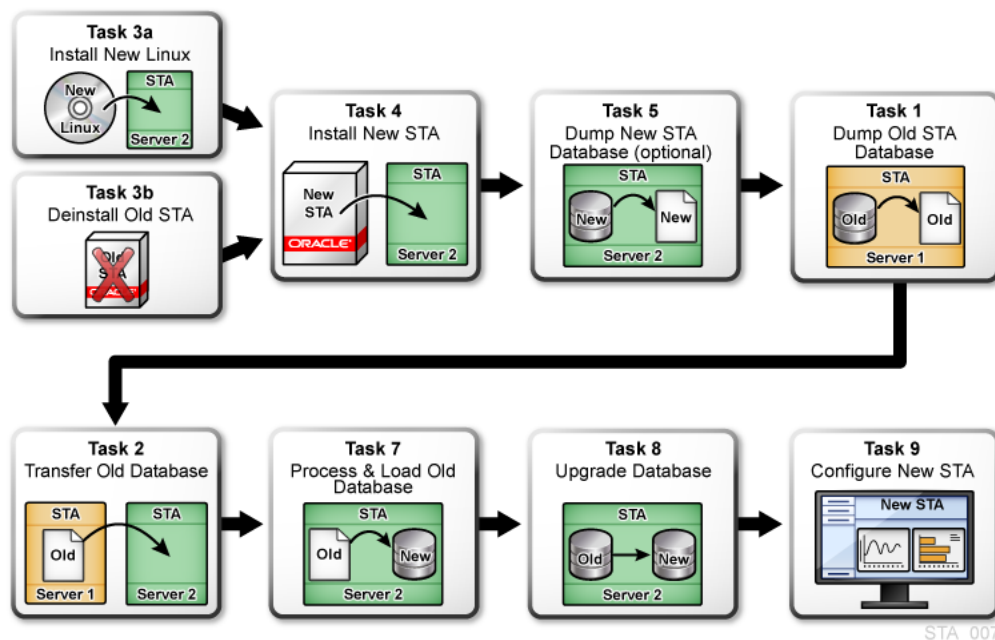
The two-server upgrade method requires a second dedicated STA server, but it offers the advantage of reduced STA application downtime. This method is especially useful if you are upgrading from STA 1.0.x, as the old version of STA can continue to monitor libraries on the old server while both Linux and the new version of STA are installed on the new server.

Even with this method, however, STA is not monitoring libraries while you upgrade the current database to the new STA version. The length of downtime depends on the size of your current database.

Figure 8–2 illustrates the two-server method. You must complete the tasks in the order shown—they are not done in sequential order, and Task 6 is omitted. Note that you do not dump the current STA database until after you install the new version of STA on the new server. In summary:

- Depending on whether the second server is currently running a version of STA, either install Linux 6.x (Task 3a) or deinstall the old version of STA (Task 3b).
- Install STA 2.2.x on the new server, and as a precaution, dump the new database (Task 4 and Task 5).
- Dump the current database on the old server and transfer it to the new server (Task 1 and Task 2).
- Load and upgrade the current database to the new STA version (Task 7 and Task 8).
- Reestablish connections to the monitored libraries and perform necessary manual configuration tasks (Task 9).

Figure 8–2 Two-server Upgrade Task Overview



Environment Changes

Review the following environment changes as part of your upgrade planning. Some or all of these changes may apply to your upgrade, depending on the version of STA you are currently running.

Linux Version

Note: This change was introduced in STA 2.1.0.

Linux 6.3 or higher is required for STA 2.1.0 and higher (see the *STA Requirements Guide* for details). You may need to install a new version of Linux as part of the STA upgrade process, as follows:

- If you are upgrading from STA 1.0.x, you must install Linux 6.3 or higher before installing STA 2.2.x. Linux does not support an in-place upgrade from Linux 5.x to Linux 6.x; instead, you must perform a new Linux 6.x installation on the STA server.
- If you are upgrading from STA 2.0.x, you are already running Linux 6.3 or higher, so you do not need to install a new version of Linux; however, you must deinstall the current version of STA before installing STA 2.2.x. 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.

Default WebLogic Port Numbers

Note: This change was introduced in STA 2.1.0.

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 higher—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.

Username and Password Requirements

Note: This change was introduced in STA 2.1.0. Additional special characters were made illegal in STA 2.2.0.

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:

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

Required Ports for STA

Note: This change was introduced in STA 2.0.0.

New dedicated STA ports were added for the StaUi and StaEngine managed servers in STA 2.0.0. 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.

Preparation Tasks for All Upgrades

Perform the following tasks before starting the STA upgrade. Most of these tasks are optional, and [Table 8–1](#) provides guidelines on when to use each one.

Table 8–1 Guidelines for When to Perform Upgrade Preparation Tasks

Task	When to Perform It
"Verify Your Site is Ready for the Upgrade" on page 8-7	All upgrades
"Save Existing Logs (optional)" on page 8-8	You want to retain service logs from the current version of STA.
"Record Current STA User and Configuration Settings (optional)" on page 8-9	You want to retain current STA usernames and configuration settings.
"Rename Custom Templates With STA- Prefix (optional)" on page 8-13	You have custom templates with names prefixed "STA-".
"Record Current Custom Template Settings (optional)" on page 8-14	You want to retain the ownership and visibility settings for existing custom templates.
"Record Executive Report Policy Settings (optional)" on page 8-14	You want to retain the ownership settings for existing Executive Report policies.

Verify Your Site is Ready for the Upgrade

Use this procedure to review the upgrade requirements and verify that your site is ready.

Verify Upgrade Prerequisites

Use this procedure to ensure that your environment meets all STA 2.2.x prerequisites.

1. Display your current STA version. Some upgrade tasks vary depending on the version of STA from which you are upgrading.
 - a. Log in to STA using an STA administrator username.
 - b. Click **About** in the Status Bar.
 - c. Verify you are running a currently released version of STA. See "[Upgrade Paths](#)" on page 8-1 for details.
2. Choose whether you will be using the single-server or two-server upgrade method. See "[Upgrade Process Overview](#)" on page 8-2 for details.
3. Verify that your site and the target server meet STA 2.2.x requirements. See the *STA Requirements Guide* for details.
4. Determine whether the /tmp filesystem 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.

If you determine you must increase the size of /tmp, you can do this just before you run the upgrade script; see ["Task 8: Upgrade the Old Database"](#) on page 8-22 for instructions.

5. Review the environment changes relevant to your upgrade path, and make any necessary adjustments to your plan or environment. See ["Environment Changes"](#) on page 8-5 for details.
6. Ensure that all required RPM packages are installed on the STA server. See ["Install Required Linux Packages"](#) on page 2-11 for instructions. As a final check, the STA installer will also notify you if any packages are missing.
7. 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 ["Recommended File System Layout"](#) on page 2-3 and ["Users, Groups, and Locations Used by the STA Installer"](#) on page 3-1.

Verify Current STA Activity

Use this procedure to verify that your current STA environment is functioning normally.

1. Use the following steps to verify that the current version of STA has had recent, successful communication with each monitored library.
 - a. Log in to STA as an STA administrator user.
 - b. From 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. Use the following steps to verify that STA is processing exchanges across all libraries.
 - a. From the **Tape System Activity** tab, select **Exchanges – Overview**.
 - b. Select the **Filter** icon and filter for Exchange End (No. Days) Less Than 1.
 - c. In the Table Toolbar, select **View**, then select **Sort**, then select **Advanced**. Sort by Drive Library Name, Drive Serial Number.
 - d. Verify that all libraries have exchange activity.

Save Existing Logs (optional)

Existing application and service logs are not retained after the upgrade because you must deinstall the current version of STA or install a new version of Linux before installing STA 2.2.x. Use this procedure to save any logs you want to keep.

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 STA File System Layout"](#) on page 2-2 for details.
2. Use the following steps to perform a service log snapshot on the current STA installation. This step is optional but recommended, as Oracle Support can use the logs to troubleshoot any issues that may have existed before the upgrade.
 - a. Log in to STA as an STA Administrator user.
 - b. From the **Setup & Administration** tab, select **Logs**.

- c. On the Service – Logs screen, click the **Create New Log Bundle** icon.
 - d. In the Create New Log Bundle dialog box, assign a bundle name and click **Save**. It may take several minutes for the process to complete.
3. Use the following steps to download the service log bundle you just created, as well as any others you want to retain. You must download the bundles one at a time.
 - a. On the Service – Logs screen, select the bundle you want to download.
 - b. Click the **Download Selected Log Bundle** icon.
 - c. In the dialog box, specify the destination location and save the log bundle.

Record Current STA User and Configuration Settings (optional)

This section applies only if you want to retain current STA usernames and configuration settings in STA 2.2.x. Use these procedures to display and record the current values so you can reenter them for STA 2.2.x. You will reenter most of these values after the upgrade; see ["Post-upgrade Tasks for All Upgrades"](#) on page 8-24 for details.

Record MySQL Usernames

Use this procedure to display and record existing MySQL usernames used to access the STA database. The STA installer will prompt you for these values. You cannot retrieve the passwords.

1. Open a terminal session on the current STA server, and log in as the system root user.
2. Display all STA database usernames by issuing the following query. Enter the database root user password when prompted. For example:

```
$ mysql -uroot -p -e "select distinct(user) from user order by user ;" mysql
Enter password: password
+-----+
| user  |
+-----+
| root  |
| staapp|
| stadb |
| starpt|
+-----+
```

3. Record the usernames.

Record STA SNMP Client Settings

Use this procedure to display and record SNMP client settings for STA. You will reenter these values after the upgrade.

Note: In the new version of STA, the SNMP values must match what is specified on the monitored libraries.

1. Log in to STA using an STA administrator username.
2. From the **Setup & Administration** tab, select **SNMP Connections**.

The Client Attributes table displays configuration settings for the STA SNMP client.

SNMP Username	Password Encryption	Privacy Encryption	Engine ID	User Community	Trap Community	SNMP Trap Le
sta1	SHA	DES	0x8000002a0500000148c730df28	public	public	1,2,3,4,11,13,14,21,25,27,41,4

3. 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, use this procedure to display and record existing WebLogic usernames used to log in to STA. You will reenter these values after the upgrade. You cannot retrieve the passwords.

Note: Starting with STA 2.0, usernames are created and maintained through the STA user interface; see "[Record STA Usernames—Upgrades From STA 2.0.x and Higher](#)" on page 8-12 for instructions.

1. Start a supported Web browser on your computer and enter the URL of the WebLogic administration console.

http(s)://STA_host_name:port_number/console/

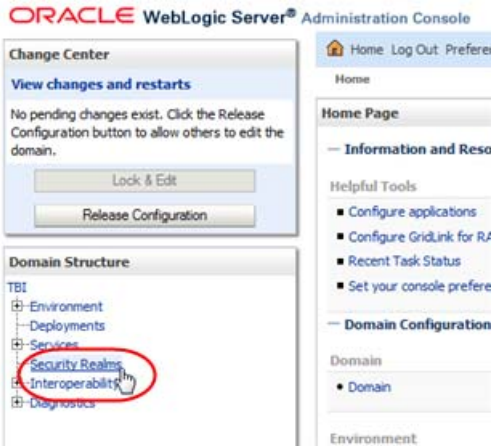
Where:

- *host_name* is the hostname of the STA server.
- *port_number* is the STA port number of the WebLogic administration console in the current STA version.
- STA must be uppercase.

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**.



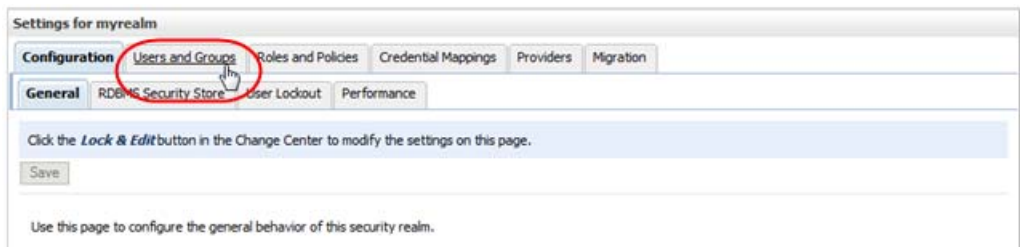
The Summary of Security Realms screen appears.

4. In the Name column, select the **myrealm** active link (do not select the check box).

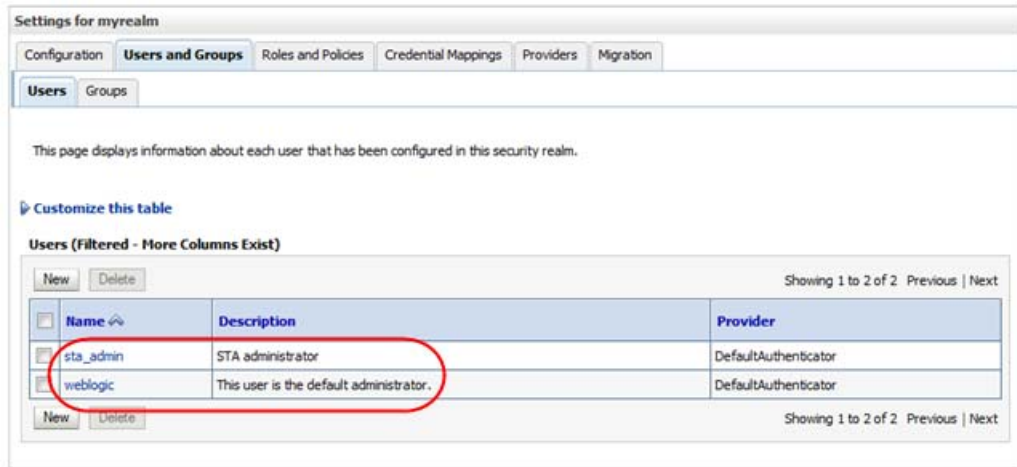


The Settings for myrealm screen appears.

5. Select the **Users and Groups** tab.



The Users table lists the available usernames.



- Record the usernames you want to retain.

Record STA Usernames—Upgrades From STA 2.0.x and Higher

For upgrades from STA 2.0.x and higher, use this procedure to display and record usernames used to log in to STA. You will reenter this information after the upgrade. You cannot retrieve the passwords.

Note: For STA 1.0.x, usernames were created and maintained through the WebLogic administration console; see "[Record WebLogic Usernames—Upgrades from STA 1.0.x Only](#)" on page 8-10 for instructions.

- Log in to STA using an STA administrator username.
- From the **Setup & Administration** tab, select **Users**.

The Configuration – Users screen displays all STA usernames and their roles.



- Record the usernames and roles you want to retain.

Record STA Email Server Settings

Use this procedure to display and record the STA email protocol and, if the email server requires authentication, the account username. You will reenter these values after the upgrade. You cannot display the password.

- Log in to STA using an STA administrator username.
- From the **Setup & Administration** tab, select **Email**.
- In the SMTP Server Settings table, select the StorageTek Tape Analytics Alerts record, then click the **Edit Selected SMTP Server** icon.

The Define SMTP Server Details dialog box appears.

4. Record the values from the following fields:
 - Use Secure Connection Protocol
 - Username

Rename Custom Templates With STA– Prefix (optional)

This procedure applies only if you have custom templates with names prefixed "STA-". During STA 2.2.x installation, all templates with the "STA-" prefix are deleted and replaced by new STA predefined templates.

Use this procedure to assign new names to the templates so they will be preserved during the upgrade.

Note: STA predefined templates are prefixed "STA-"; therefore Oracle recommends that you *not* use this prefix when naming custom templates.

1. Log in to STA with an administrator username.
2. From 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-".
You are taken to the screen with the selected template applied.
5. Click **Save Template** in the Templates Toolbar.
The Save Template dialog box appears.
6. In the **Template Name** field assign a new name not prefixed "STA-". Your entry must be unique.
7. Click **Save**.

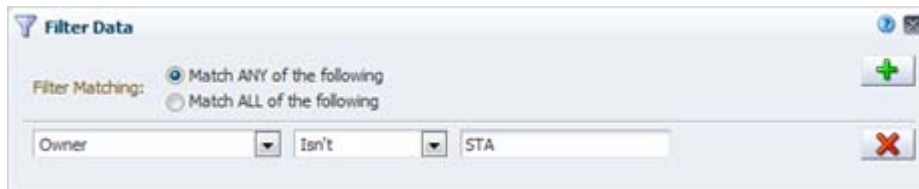
The template is saved.

Record Current Custom Template Settings (optional)

This section applies only if you have custom templates. The upgrade preserves custom templates, but after the upgrade all custom templates are owned by STA with public visibility.

Use this procedure to record the current ownership and visibility settings for all custom templates so you can restore them after the upgrade, if necessary. You can skip this procedure if template ownership and visibility are not critical to your implementation.

1. Log in to STA with an administrator username.
2. From the **Setup & Administration** tab, select **Templates Management**.
3. Select the **Filter** icon and filter the screen to show only templates not owned by STA—this will display custom templates only.



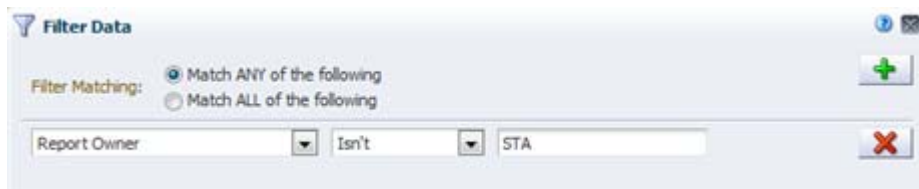
4. Record the current Owner and Public Visibility settings for each custom template. If you have many templates, you may want to take a screen shot.

Record Executive Report Policy Settings (optional)

This section applies only if you have privately owned Executive Report policies. The upgrade preserves all Executive Report policies, but after the upgrade all private policies 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. Select the **Filter** icon and filter the screen to show only policies not owned by STA—this will display private policies only.



4. Record the current Report Owner for each policy. If you have many policies, you may want to take a screen shot.

Post-installation Upgrade Tasks

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.

If you are using the single-server upgrade method, you perform the tasks in sequential order; see [Figure 8-1, "Single-server Upgrade Task Overview"](#) for details.

If you are using the two-server upgrade method, you do *not* perform the tasks in sequential order and Task 6 is omitted; see [Figure 8-2, "Two-server Upgrade Task Overview"](#) for the task order.

- ["Task 1: Dump the Old STA Database"](#) on page 8-15
- ["Task 2: Transfer the Old Database Dump"](#) on page 8-16
- ["Task 3a: Install the New Linux Version—Upgrades From STA 1.0.x"](#) on page 8-17
- ["Task 3b: Deinstall the Old STA Version—Upgrades From STA 2.0.x or Higher"](#) on page 8-17
- ["Task 4: Install the New STA Version"](#) on page 8-18
- ["Task 5: Dump the New STA Database \(optional\)"](#) on page 8-19
- ["Task 6: Transfer the Old STA Database to the STA Server"](#) on page 8-20
- ["Task 7: Process and Load the Old STA Database"](#) on page 8-20
- ["Task 8: Upgrade the Old Database"](#) on page 8-22
- ["Post-upgrade Tasks for All Upgrades"](#) on page 8-24
- ["Recover a Failed Database Upgrade \(optional\)"](#) on page 8-23

Task 1: Dump the Old STA Database

Use this procedure to perform a full dump of the old (current) STA database.

1. Use the following steps to display the size of your current STA database.
 - a. Log in to STA using an STA administrator username.
 - b. Click **About** in the Status Bar.
 - c. In the About dialog box, scroll down to where the Database Current Size is displayed, and record the value.
2. Use the following steps to verify that the location where you want to dump the database has sufficient space.
 1. Open a terminal session on the STA server and log in as the system root user.
 2. 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
```

3. Stop all STA services.

```
# STA stop all
```

4. Start the MySQL service.

```
# service mysql start
```

5. Dump the STA database into a single file. 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
```

Note: The optional `-v` parameter (for verbose output) is not recommended, as a large number of messages are displayed in the terminal window and it can significantly slow down the command process for large databases.

In [Example 8-1](#), the STA 1.0.x database is dumped into the `/dbdumpfiles` folder on the STA server with filename `Dec14_dump.sql`.

Example 8-1 Old Database Dump

```
# mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert
--dump-date --events --flush-logs --routines --single-transaction --triggers
--databases stadb > /dbdumpfiles/Dec14_dump.sql
```

```
Enter password: mysql_root_password
```

```
...
-- Retrieving view structure for table v_library_complex_io...
...
-- Retrieving view structure for table v_library_summary_averages...
-- It's base table, skipped
...
-- Retrieving table structure for table v_mdv_status_codes...
-- It's a view, create dummy table for view
...
-- Disconnecting from localhost...
```

6. To reduce the dump file size by approximately 50 percent, gzip the file.

```
# cd /path_to_dump_file/
# gzip dump_file_name.sql
```

Task 2: Transfer the Old Database Dump

Use this procedure to transfer the compressed dump of the old STA database to either an off-platform backup server (single-server method) or the new STA 2.2.x server (two-server method).

Caution: If you are upgrading from STA 1.0.x with the single-server method, you must back up the STA database to another server. Do not back up the database to a filesystem on the current STA server, as the Linux 6.x installation in "[Task 3a: Install the New Linux Version—Upgrades From STA 1.0.x](#)" on page 8-17 will destroy all data on the server.

1. If you have not done so already, stop all STA services.

```
# STA stop all
```

2. Perform a checksum before transferring the file to the backup server.

```
# cksum dump_file_name.sql.gz
```

The output includes a checksum value and byte count. Record the checksum value; you will use it to verify the file integrity after transferring the file to the backup server.

3. Transfer the file to the target server using a transfer utility such as SCP. The `-p` option preserves timestamp values.

```
# scp -p dump_file_name.sql.gz target_host:/path/
```

In [Example 8–2](#), SCP is used to transfer the compressed database dump file `Dec14_dump.sql.gz` to the `/dbdumpfiles` folder on backup host `backup1`. The `/dbdumpfiles` folder already exists on the backup host.

Example 8–2 Old Database Transfer to Backup Server (Single-server Method)

```
# cd /dbdumpfiles
# scp -p Dec14_dump.sql.gz backup1:/dbdumpfiles
```

In [Example 8–3](#), SCP is used to transfer the compressed database dump file `Dec14_dump.sql.gz` to the `/dbdumpfiles` folder on STA 2.2.x host `sta_new`.

Example 8–3 Old Database Transfer to New STA Server (Two-server Method)

```
# cd /dbdumpfiles
# scp -p Dec14_dump.sql.gz sta_new:/dbdumpfiles
```

4. On the target server, perform a checksum of the transferred file. Verify that the checksum values match.

```
# cd /path_to_dump_file/
# cksum dump_file_name.sql.gz
```

Task 3a: Install the New Linux Version—Upgrades From STA 1.0.x

Caution: This activity destroys all data on the server. If you are using the single-server upgrade method, use this procedure only after you have performed "[Task 1: Dump the Old STA Database](#)" on page 8-15 and "[Task 2: Transfer the Old Database Dump](#)" on page 8-16.

This procedure applies only to upgrades from STA 1.0.x. Install Linux 6.3 or higher on the STA server; see [Chapter 2, "Installing Linux"](#) for instructions.

Task 3b: Deinstall the Old STA Version—Upgrades From STA 2.0.x or Higher

Caution: This activity destroys all STA data on the server. If you are using the single-server upgrade method, use this procedure only after you have performed "[Task 1: Dump the Old STA Database](#)" on page 8-15 and "[Task 2: Transfer the Old Database Dump](#)" on page 8-16.

This procedure applies only to upgrades from STA 2.0.x or higher. Deinstall the current version of STA, as follows. The location of the deinstaller varies depending on the version of STA.

- For upgrades from STA 2.1.x and higher, see ["Deinstall STA"](#) on page 9-2 and ["Verify Successful Deinstallation"](#) on page 9-2 for instructions.
- For upgrades from STA 2.0.x, use the following steps.

1. Log in as the system root user.

2. Change to the STA installation directory.

```
# cd /Oracle/StorageTek_Tape_Analytics_install
```

3. Launch the STA deinstaller with one of the following commands:

- To use the STA graphical deinstaller:

```
# ./Uninstall_StorageTek_Tape_Analytics
```

This mode requires an X11 display. See ["STA Graphical Installer and Deinstaller Screen Reference"](#) on page A-1 for instructions.

- To use the STA console deinstaller:

```
# ./Uninstall_StorageTek_Tape_Analytics -i console
```

Task 4: Install the New STA Version

Use this procedure to install STA 2.2.x.

1. Install STA 2.2.x; see ["Installing STA"](#) on page 3-1 for instructions.
2. To verify STA is working properly and complete the STA Administrator setup in WebLogic, log in to the STA application.

The Dashboard is displayed.

Note: Because the upgrade process is not yet complete, the Dashboard portlets display the message "No data to display"; this is normal. The library data will be displayed correctly after you upgrade the database and configure the new STA version.

3. Log out of STA.

4. Open a terminal session on the STA server and log in as the system root user.

5. Stop all STA services.

```
# STA stop all
```

6. This step applies only if you want STA to monitor the libraries using SNMP v2c (see [Appendix F, "Configuring SNMP v2c Mode"](#) for details). Starting with STA 2.0, SNMP v2c is enabled by default. Use the following steps to confirm that it is enabled.

- a. Change to the STA configuration files directory.

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


- b. Display the SNMP version properties file and verify that the V2c parameter is set to true.

```
# cat TbiSnmpVersionSupport.properties
V2c=true
Verbal=false
```

- c. If the parameter is not set to true, see ["Enable SNMP v2c Mode for STA"](#) on page F-3 for instructions on how to change it.

Task 5: Dump the New STA Database (optional)

This procedure is optional but recommended. Use this procedure to dump the empty STA 2.2.x database as a safeguard. If the database upgrade ([Task 8: Upgrade the Old Database](#)) cannot be completed, you can restore the empty database to recover STA 2.2.x to a state in which it can be configured to run as if it were newly installed with no data; see [Recover a Failed Database Upgrade \(optional\)](#) for details on the recovery process.

1. Open a terminal session on the STA server and log in as the system root 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. 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
```

Note: The optional `-v` parameter (for verbose output) is not recommended, as a large number of messages are displayed in the terminal window and it can significantly slow down the command process for large databases.

In [Example 8-4](#), the STA 2.2.x database is dumped to the `/dbdumpfiles` folder on the STA server with filename `STA_FRESH_INSTALL_BACKUP.sql`.

Example 8-4 New Database Dump

```
# mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert
--dump-date --events --flush-logs --routines --single-transaction --triggers
--databases stadb > /dbdumpfiles/STA_FRESH_INSTALL_BACKUP.sql
Enter password: mysql_root_password
...
-- Retrieving view structure for table v_mdv_request_states...
-- Retrieving view structure for table version_info...
...
-- Disconnecting from localhost...
```

Note: If you see the message, "Can't connect to local MySQL server," the MySQL server is not running. Make sure you have started MySQL (Step 3).

Task 6: Transfer the Old STA Database to the STA Server

Note: This procedure applies to the single-server method only.

Use this procedure to transfer the backup of the old database to the STA 2.2.x server.

1. If you have not done so already, stop all STA services.

```
# STA stop all
```

2. 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 [Example 8-5](#), SCP is used to transfer the compressed database dump file `Dec14_dump.sql.gz` from `/dbdumpfiles` on host `backup1` to the `/dbdumpfiles` folder on the STA 2.2.x server.

Example 8-5 Old Database Transfer to New STA Server

```
# scp -p backup1:/dbdumpfiles/Dec14_dump.sql.gz /dbdumpfiles
```

3. Perform a checksum of the transferred file. Verify the checksum value matches the one you received in "[Task 1: Dump the Old STA Database](#)" on page 8-15.

```
# cd /path_to_dump_file/  
# cksum dump_file_name.sql.gz
```

Task 7: Process and Load the Old STA Database

Use this procedure to decompress the old database and reinstate it on the STA 2.2.x server. The decompressed database may require 10 to 15 times as much space as the compressed database.

1. If you have not done so already, stop all STA services.

```
# STA stop all
```

2. Decompress the backup file.

```
# gunzip dump_file_name.sql.gz
```

3. Use the following steps to 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.

```
# ./purgerecs /path_to_dump_file/dump_file_name.sql /path_to_dump_
file/dump_file_name_PURGED.sql
```

Note: For help with the `purgerecs` command, type the following command:

```
# ./purgerecs -h
```

In [Example 8–6](#), the `purgerecs` utility processes the MySQL dump file `Dec14_dump.sql` in `/dbdumpfiles`. The output is directed to a new file named `Dec14_dump_PURGED.sql` in `/dbdumpfiles`. A progress dot appears for each 200 records processed.

Example 8–6 Purge Obsolete Data From the Old Database Backup

```
# cd /Oracle/StorageTek_Tape_Analytics/db/updates
# ./purgerecs /dbdumpfiles/Dec14_dump.sql /dbdumpfiles/Dec14_dump_PURGED.sql
```

```
.....
          STA v1.0.2, Schema 33.02
Processed 11,689 lines from '20130711_dump.sql':
-----
snmp_storage_cells.....1,614,255
snmp_media.....110,205
...
media_summaries.....254
transform_logs.....0
=====
Records Processed:.....13,143,283
Records Purged:.....2,857,623
Records Remaining:.....10,285,660
Elapsed Time:.....00:00:11
```

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. Enter the database root user password when prompted. Unless you specify the `-v` (verbose) option (not recommended), there is no command output as the process runs.

Note: The optional `-v` parameter (for verbose output) is not recommended, as a large number of messages are displayed in the terminal window and it can significantly slow down the command process for large databases.

```
# 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.

Task 8: Upgrade the Old Database

Use this procedure to upgrade the old STA database to the new STA 2.2.x schema.

1. If you have not done so already, stop all STA services.

```
# STA stop all
```

2. If you determined in "[Verify Upgrade Prerequisites](#)" on page 8-7 that the size of `/tmp` is not sufficient for the upgrade, increase the size of `/tmp` as necessary.

If this is not possible, use the following steps to 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, and enter the database root user password when prompted. For security reasons, the password is not displayed on the screen.

```
# ./upgradedb.sh
```

Note: You can perform this step as either the system root user or the Oracle install user.

Following is an example of the screen display.

```
# ./upgradedb.sh
```

```
DB Root Password:
```

```
+-----+
| STA DATABASE UPGRADE                               |
| Upgrading DB schema from 58.00r0 to 59.00r0        |
| Started: 2014-12-12 15:14:45                       |
+-----+
STA database is 5.15 GB and contains approximately 12,636,002 records.
Checking if current database v58.00 is a valid upgrade candidate...
...DB v58.00 is a valid upgrade candidate...
+-----+
==> You may ABORT using CTRL-C within 7 seconds
==> .....6.....5.....4.....3.....2.....1
==> CTRL-C disabled!
+-----+
Starting upgrade...
```

When the process is complete, a banner similar to the following is displayed.

Caution: Wait until you see this banner before proceeding.

```
+-----+
| Started.....2014-12-12 15:14:45                    |
| Finished.....2014-12-12 17:07:11                   |
| Elapsed Time.....01:52:26                          |
| Starting Version.....58.00r0                       |
| Final Schema Version....59.00r0                    |
| Schema Release Date....2014-12-12 11:00:00         |
| Records (approximate)...12,636,002                 |
+-----+
```

5. If in "[Task 8: Upgrade the Old Database](#)" on page 8-22 you increased the size of /tmp or created an alternate temp location, restore it to its normal size and location.
6. Start all STA services.

```
# STA start all
```
7. This step is optional. Delete the STA_FRESH_INSTALL_BACKUP.sql file to free up disk space on the STA database backup volume.

Recover a Failed Database Upgrade (optional)

Caution: Perform this procedure only under the direction of your Oracle support representative.

Use this procedure only if the database upgrade in ["Task 8: Upgrade the Old Database"](#) on page 8-22 does not complete successfully and attempts to repeat the upgrade have also failed.

1. Repeat ["Task 7: Process and Load the Old STA Database"](#), Step 6, through ["Task 8: Upgrade the Old Database"](#).

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.

2. Delete the damaged upgraded database.

```
# mysql -uroot -p -e "drop database stadb;"
```

3. Change to the STA database backup location and load the new installation database dump file you created in ["Task 5: Dump the New STA Database \(optional\)"](#) on page 8-19.

For example:

```
# cd /dbbackup
# mysql -uroot -p -e < /home/oracle/STA_FRESH_INSTALL_BACKUP.sql
```

4. Perform ["Task 8: Upgrade the Old Database"](#) on page 8-22.
5. Configure STA as a new installation. See the following sections for details:
 - ["Configuring Library Connections in STA"](#) on page 6-1
 - ["Configuring STA Services"](#) on page 7-1

Post-upgrade Tasks for All Upgrades

Use these procedures to configure the libraries and STA 2.2.x so STA can begin monitoring library activity.

- ["Update the STA Trap Recipient on the Libraries"](#) on page 8-24
- ["Configure SNMP Settings in STA"](#) on page 8-25
- ["Configure STA Services and User Information"](#) on page 8-26
- ["Decommission the Old STA Server \(optional\)"](#) on page 8-26

Update the STA Trap Recipient on the Libraries

Two new trap levels, 13 (Test Trap) and 14 (Health Trap), were introduced in STA 2.0. Proceed as follows depending on your upgrade path:

- If you are using the two-server upgrade method, add the new STA 2.2.x server as a trap recipient on each monitored library, and be sure to include the new trap levels in the definition. See ["Create the STA SNMP v3 Trap Recipient"](#) on page 5-8 or ["Create the STA SNMP v2c Trap Recipient on the Library"](#) on page F-2.
- If you are using the single-server method to upgrade from STA 2.0.x or higher, 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 SNMP Settings in STA"](#) on page 8-25.
- 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.

Note: For all library models except SL150, to modify a trap recipient, you must delete the existing definition and then add a new one.

All libraries except SL150

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
```

Where:

- *index* is the index number of the 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](#)" on page 5-8 or "[Create the STA SNMP v2c Trap Recipient on the Library](#)" on page F-2 for instructions.

SL150 libraries

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 SNMP Settings in STA

Perform these steps for all upgrades. These steps are performed in STA.

1. Log in to STA as an STA administrator user.
2. Reenter the configuration settings for the STA SNMP client, using the values you recorded before the upgrade; see "[Record Current STA User and Configuration Settings \(optional\)](#)" on page 8-9. These values must match what is configured on the monitored libraries. See "[Configure SNMP Client Settings for STA](#)" on page 6-4 for instructions.
3. To restore SNMP communication between STA and the libraries, test the connection to each monitored library. See "[Test a Library SNMP Connection](#)" on page 6-7 for instructions.

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.

4. Get the latest SNMP library configuration data from each library. See ["Perform a Manual Data Collection"](#) on page 6-9 for instructions.

Configure STA Services and User Information

Perform these steps for all upgrades. These steps are performed on the STA server.

If you want to retain settings from the previous STA version, use the values you recorded before the upgrade; see ["Record Current STA User and Configuration Settings \(optional\)"](#) on page 8-9.

Note: After the upgrade, all logical groups are owned by STA. Logical group ownership is not critical to STA functioning, and any STA user with Operator or Administrator privileges can modify logical groups.

1. Configure the STA Backup service and STA Resource Monitor service utilities. See [Chapter 7, "Configuring STA Services"](#) for details.
2. Create STA usernames and passwords; see the *STA User's Guide* for instructions. You may also want to do the following:
 - Notify users of the new password requirements for STA 2.2.x.
 - Direct users to reenter their custom user preferences, if applicable.
3. If the STA email server requires authentication, you must enter the email account username and password; see the *STA User's Guide* for instructions.
4. Restore original ownership to custom templates, as applicable; see the *STA User's Guide* for instructions.
5. Restore original ownership to private Executive Report policies, as applicable; see the *STA User's Guide* for instructions.

Decommission the Old STA Server (optional)

This procedure applies only if you used the two-server post-installation upgrade method. You can use this procedure 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 the *STA User's Guide* for instructions.
2. Decommission the old STA server.

Deinstalling and Restoring STA

This chapter includes the following sections:

- [STA Deinstallation Overview](#)
- [STA Deinstallation Tasks](#)

Caution: Oracle does not support downgrading STA to a prior version. Database data created with a newer version of STA will be lost when installing an older version of STA.

STA Deinstallation Overview

The STA deinstaller removes the STA application and all associated data and Oracle software. The following updates are made.

- 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 STA File System Layout](#)" on page 2-2 for details about this location.
- All STA service logs are removed.
- The STA database 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](#)" for details.

The STA deinstaller is available in both graphical and silent modes. See "[STA Installer Modes](#)" on page 3-7 for details.

See "[STA Installation and Deinstallation Logs](#)" on page 3-6 for details about the STA deinstallation logs.

STA Deinstallation Tasks

The following sections describe how to use the STA deinstaller.

- ["Deinstall STA"](#) on page 9-2
- ["Verify Successful Deinstallation"](#) on page 9-2
- ["Restore STA"](#) on page 9-3

Deinstall STA

Use this procedure to deinstall STA.

Caution: Deinstallation removes all STA database data. Before starting this procedure, you should perform a full database dump. See ["Task 1: Dump the Old STA Database"](#) on page 8-15 for instructions.

Note: To deinstall STA, you must log in as a user that is a member of the Oracle install group. You cannot deinstall STA as the Linux root user nor any other user with superuser privileges. See ["Oracle install group"](#) for details.

1. Log in as the Oracle install user.
2. Change to the STA home directory. For example:

```
$ cd /Oracle/StorageTek_Tape_Analytics
```
3. Change to the STA installer binary directory.

```
$ cd oui/bin
```
4. Launch the STA deinstaller with one of the following commands:

- To use the STA graphical deinstaller:

```
$ ./deinstall.sh
```

This mode requires an X11 display. See ["STA Graphical Installer and Deinstaller Screen Reference"](#) on page A-1 for instructions.

- To use the STA silent deinstaller:

```
$ ./deinstall.sh -silent -responseFile response_file
```

Where *response_file* is the absolute path of the previously created response file.

Before using this mode, you must also download the `silentInstallUtility.jar` file and create a response file specifying the deinstallation options. See [Appendix B, "STA Silent-mode Installer and Deinstaller"](#) for instructions.

Verify Successful Deinstallation

Use this procedure to verify that all STA components have been removed from the STA server after deinstallation.

1. Log in as the Oracle install user.
2. List 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 ..
$
```

Restore STA

Use this procedure to deinstall and then reinstall STA—for example, to repair a current installation. You cannot use the STA installer to reinstall or overwrite a current installation.

1. Perform a service log snapshot on the current STA installation. Oracle Support can use the generated service logs to troubleshoot any issues that may have existed before the restoration. See the *STA User's Guide* for detailed instructions.

2. Stop all STA services:

```
# STA stop all
```

3. Perform a database snapshot.

- a. Start the MySQL service.

```
# STA start mysql
```

- b. Create a backup file.

```
# /usr/bin/mysqldump -uroot -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 isn't running. Return to Step a and verify you have started MySQL.

4. Move the service log snapshot and database snapshot to another server, as all STA files will be removed in the next step. The snapshots are located in the following directories:

- The service log snapshot is in */Oracle_storage_home/Middleware/rda/snapshots*. For example, */Oracle/Middleware/rda/snapshots*
- The database snapshot is in the database location specified during STA installation. For example, */dbbackup*

5. Back up other files as needed.

6. Deinstall STA. See "[Deinstall STA](#)" on page 9-2. for instructions.

7. Re-install STA. See [Chapter 3, "Installing STA."](#) for instructions.

8. Stop all STA services:

```
# STA stop all
```

9. Restore the database. See the *STA Administration Guide* for instructions.
10. Start all STA services:

```
# STA start all
```
11. Configure STA. See "[Configure SNMP Settings in STA](#)" on page 8-25 for instructions.

STA Graphical Installer and Deinstaller Screen Reference

This chapter includes the following sections:

- [Graphical-mode Display Requirements](#)
- [STA Graphical Installer Screens](#)
- [STA Graphical Deinstaller Screens](#)

Graphical-mode Display Requirements

The STA graphical-mode installer and deinstaller require X Window System, version 11 (X11). X11 configuration is outside the scope of this guide; however, the following general guidelines apply. For additional information, contact your system administrator.

For you to run the graphical-mode installer and deinstaller, the X11 service must be running on the STA server and configured to allow X11 forwarding. If Linux was installed as instructed in [Chapter 2, "Installing Linux,"](#) these conditions should already be met.

In addition, X11 authorizations and display must be set correctly for the Oracle install user. This is handled differently depending on whether you are logging in through a local or remote connection.

See the following sections for details.

- ["Local Connections"](#) on page A-1
- ["Remote Connections Using a Secure Shell \(SSH\)"](#) on page A-2
- ["Remote Connections Using Desktop Sharing"](#) on page A-2
- ["Troubleshooting Graphical Display Issues"](#) on page A-3

Note: Response time for remote connections depends on your network and VPN configurations and performance.

Local Connections

For direct connections to the STA server, you must log in as the Oracle install user and then set the DISPLAY variable manually. For example:

```
# export DISPLAY=hostname:0.0
```

You may also need to verify that the Oracle install user has the proper X11 authorization. Contact your Linux administrator for assistance.

Remote Connections Using a Secure Shell (SSH)

If you use a secure shell (SSH) with X11 forwarding enabled, X11 authorization and display are handled automatically for the login user. For example, if you use this method and log in as the oracle user, the SSH service on the STA server automatically sets up the proper X11 authorization and display for the oracle user. You should not set the DISPLAY variable manually.

However, if you log in as a different user (root, for example) 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.

Connecting From a Linux Machine

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
```

Connecting From a Microsoft Windows PC

Your PC must be running an X11 server, such as Xming or Cygwin/X, and an SSH client, such as PuTTY or WinSCP. Following is a sample procedure for connecting using PuTTY:

1. Verify that the X11 server is running on your PC. Contact your system administrator for assistance, if necessary.
2. Start PuTTY, and proceed as follows:
 - a. 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**.
 - b. 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.

Remote Connections Using Desktop Sharing

To run the STA installer through desktop sharing, both the STA server and your local computer must be running a desktop sharing application, such as VNC Server on the STA server and VNC Viewer on your local computer. In addition, your local computer must be able to connect to the STA server through a private network, such as Virtual Private Network (VPN).

Following is a sample process for connecting using VNC.

1. Install and configure the VNC Server on the STA server.
2. Install and configure the VNC Viewer on your local computer.

3. Connect to the STA server through the private network. Contact your IT administrator for instructions.

Troubleshooting Graphical Display Issues

The STA installer and deinstaller verify that X11 is properly configured for the Oracle install user. If these prerequisite checks fail, contact your Linux system administrator for assistance. You can use the following steps to help troubleshoot problems.

1. Log in to the STA server as the Oracle install 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 the Oracle install user. For example:

```
$ echo $DISPLAY
:0.0
```

3. Verify the display has the proper X11 configuration. For example:

```
$ xdpinfo -display :0.0
```

[Example A-1](#) is a sample of the first part of the command output showing a properly configured display.

Example A-1 Sample Properly Configured X11 Display

```
$ xdpinfo
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 A-2](#) shows some examples of the command output from displays that are not configured correctly.

Example A-2 Sample Improperly Configured X11 Displays

```
$ xdpinfo
xdpinfo: unable to open display ":0.0".

$ xdpinfo
PuTTY X11 proxy: MIT-MAGIC-COOKIE-1 data did not matchxdpinfo: unable to open
display ":0.0".
```

STA Graphical Installer Screens

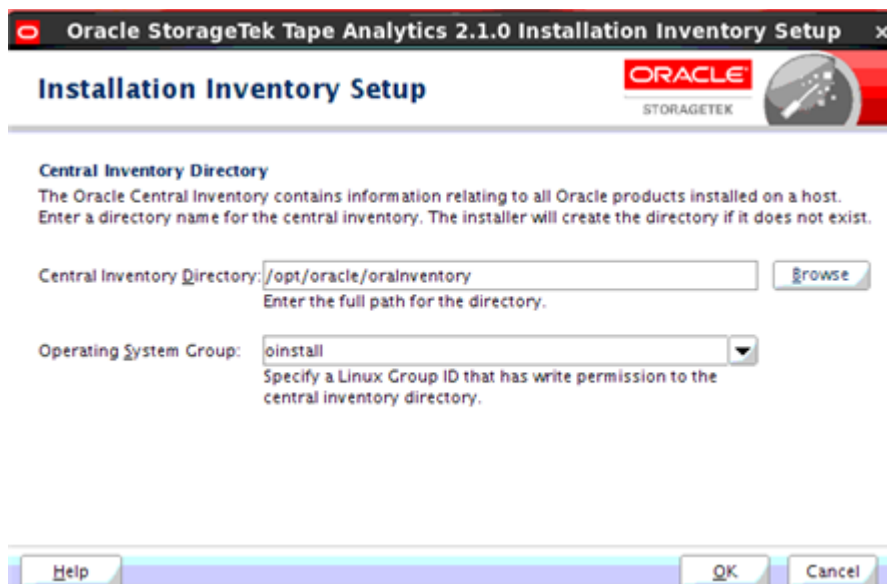
This section provides detailed reference for each screen of the STA graphical installer.

- ["Welcome"](#) on page A-6
- ["Installation Location"](#) on page A-8

- "Prerequisite Checks" on page A-10
- "Enter Root Password" on page A-14
- "Set Up DB Directories" on page A-15
- "Set Up Admin Accounts" on page A-16
 - "WebLogic Administrator" on page A-17
 - "STA Administrator" on page A-18
- "Set Up Database Accounts" on page A-19
 - "Database Root User" on page A-20
 - "Database Application User" on page A-21
 - "Database Reports User" on page A-22
 - "Database Administrator" on page A-23
- "Enter Communication Ports" on page A-24
 - "WebLogic Admin Console" on page A-25
 - "STA Engine" on page A-26
 - "STA Adapter" on page A-27
 - "STA UI" on page A-28
- "Diagnostic Agent" on page A-29
- "Installation Summary" on page A-30
- "Installation Progress" on page A-31
- "Configuration Progress" on page A-33
- "Installation Complete" on page A-35

Note: When you launch the STA graphical installer, the Oracle Universal Installer displays messages in the terminal window as it performs some basic environment checks. Requirements for running the STA graphical installer may exceed these minimal checks.

Installation and Inventory Setup



This screen is part of the Oracle Universal Installer. The Oracle central inventory directory is used to keep track of the names and locations of all Oracle software installed on this server. All STA installation and deinstallation logs are saved automatically to this location.

If you follow the recommended practices for registering the Oracle central inventory, this screen appears only the first time you install STA on this server, and subsequent installations and upgrades automatically find the location without prompting you. See ["Register the Oracle Central Inventory Location"](#) on page 3-19 for details.

If this screen appears after STA has already been installed at least once, either the Oracle central inventory was not registered, or the inventory pointer file has been deleted. See ["Display the Oracle Central Inventory Location"](#) on page 3-19 for instructions on determining the correct location to enter.

Screen Fields

Inventory Directory

Enter the full path to the Oracle central inventory directory. To ensure that other users in the Oracle install group have access to this directory, it should be separate from the Oracle install user's home directory. Home directories may not have proper permissions for the Oracle install group.

The default is `$USER_HOME/orainventory`. You must specify an absolute path, or click the **Browse** button to navigate to an existing directory.

- If you specify an existing directory, the Oracle install user must have full permissions to it.
- If you specify a directory that does not exist, the installer will create it automatically if the Oracle install user has full permissions to the parent directory.

Operating System Group

Select the Linux group you want to designate as the Oracle install group. All members of this group will be able to install Oracle software on this server.

The menu lists all groups to which the Oracle install user belongs. The default is the Oracle install user's primary group.

Screen-specific Buttons

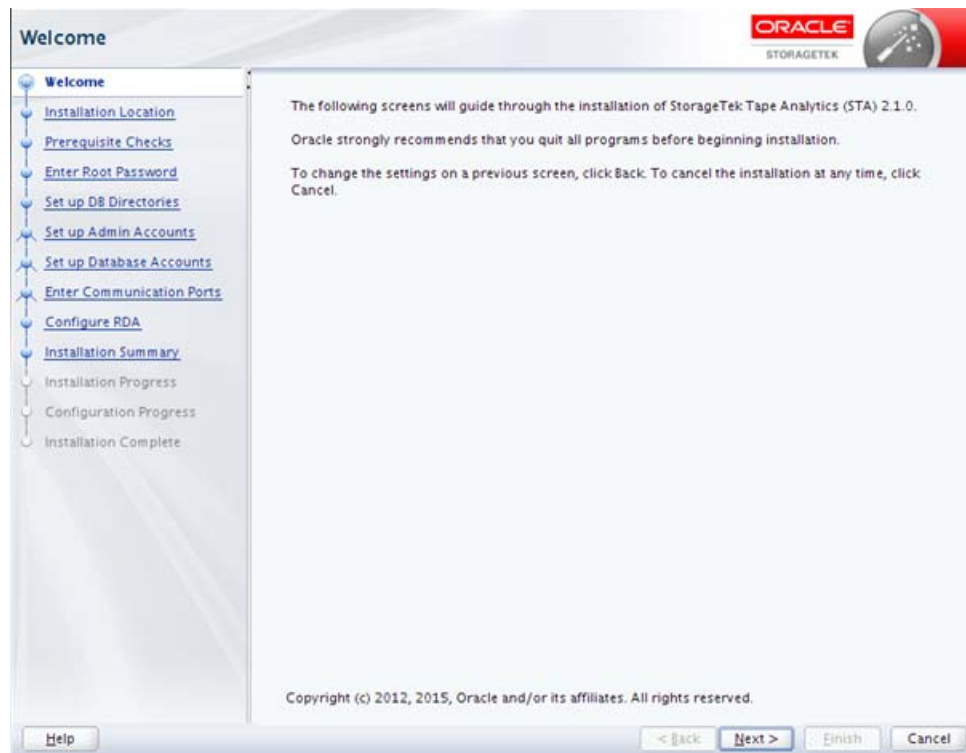
Browse

Click to navigate to the directory you want to specify.

OK

Click to initiate the STA installer. The Installation Inventory Setup window disappears and there may be a slight delay before the STA Installer Splash Screen appears.

Welcome



This screen provides some general information for running the STA installer. Read the text, then click **Next** to begin the installation.

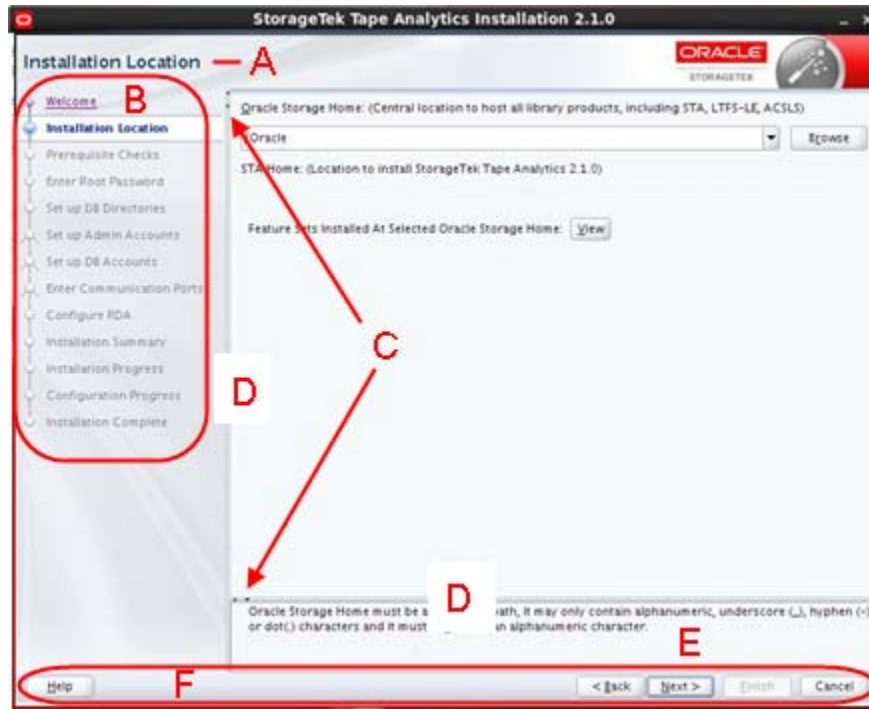
If the installer detects an instance of STA anywhere on the server, it does not allow you to continue. To install STA 2.2.x, you must perform a manual post-installation upgrade. See "[Upgrading to STA 2.2.x](#)" on page 8-1 for instructions.

Note: System changes are not implemented until you have completed all the STA installer input screens and clicked **Install** in "[Installation Summary](#)" on page A-30. Anytime before then, you can return to a previous screen and modify your entries.

See "[General Installer Screen Layout](#)" on page A-7 for details about the STA installer screens.

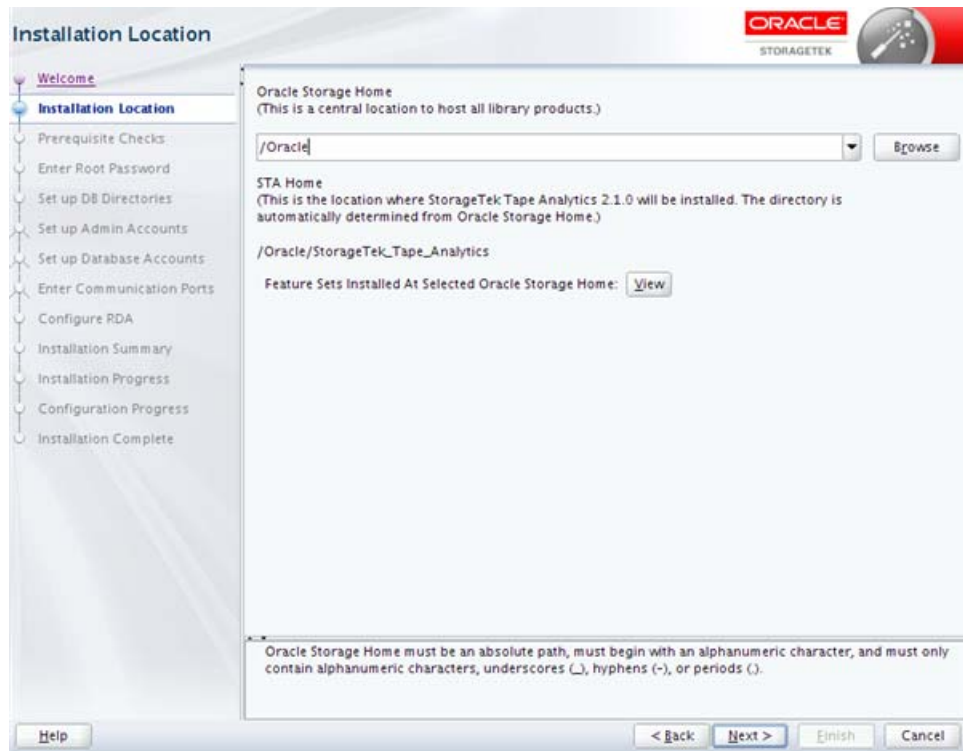
General Installer Screen Layout

All STA installer screens follow the same basic layout. The main parts are illustrated and described below.



Item	Name	Description
A	Screen title	Title of the STA installer screen
B	Navigation tree	Displays your current position in the installation sequence. Screen titles become active links as you complete each screen. You can click any active link to return directly to that screen and review or change your entries
C	Expand and Collapse icons	Click to hide or display the Navigation tree and the Message pane.
D	Resize control bar	Click and drag to resize the Navigation tree or the Message pane.
D	Message pane	Included only on selected screens. Displays status messages relevant to processes performed on that screen.
E	Common buttons	The following buttons are common to all STA Installer screens: <ul style="list-style-type: none"> ■ Help—Click to display context-sensitive help for the screen. ■ Back—Click to go to the previous screen to review or change your entries. You can go back one screen at a time to the beginning of the installation. ■ Next—Click to proceed to the next screen after making the necessary entries. ■ Finish—Click to complete the installation. This button is active only for the final screen. ■ Cancel—Click to cancel the installation at any time. If any part of the installation has been performed, the installer will roll back the installation and return the server to its original state. You will be prompted to confirm the cancellation.

Installation Location



This screen allows you to specify the location where STA and associated Oracle software will be installed on the server.

To determine whether STA has already been installed in a particular location, you can enter a directory in the **Oracle Storage Home** field and click the **View** button.

- If no STA software has been installed in that location, the list is blank.
- If STA software has been installed, it is listed as shown in [Figure A-1, "Sample Listing of Oracle Storage Home"](#).

Screen Fields

Oracle Storage Home

Enter the directory where STA and associated Oracle software will be installed. Each software package will be installed in its own subdirectory within this directory.

See [Table 2-1, "Recommended File System Layout"](#) for technical recommendations about this directory.

Depending on whether this directory already exists, the Oracle install user and group must have the following permissions:

- If the directory does exist, 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.

You must enter an absolute path, or click the **Browse** button to navigate to the directory you want to specify.

STA Home

Display only. 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.

Screen-specific Buttons

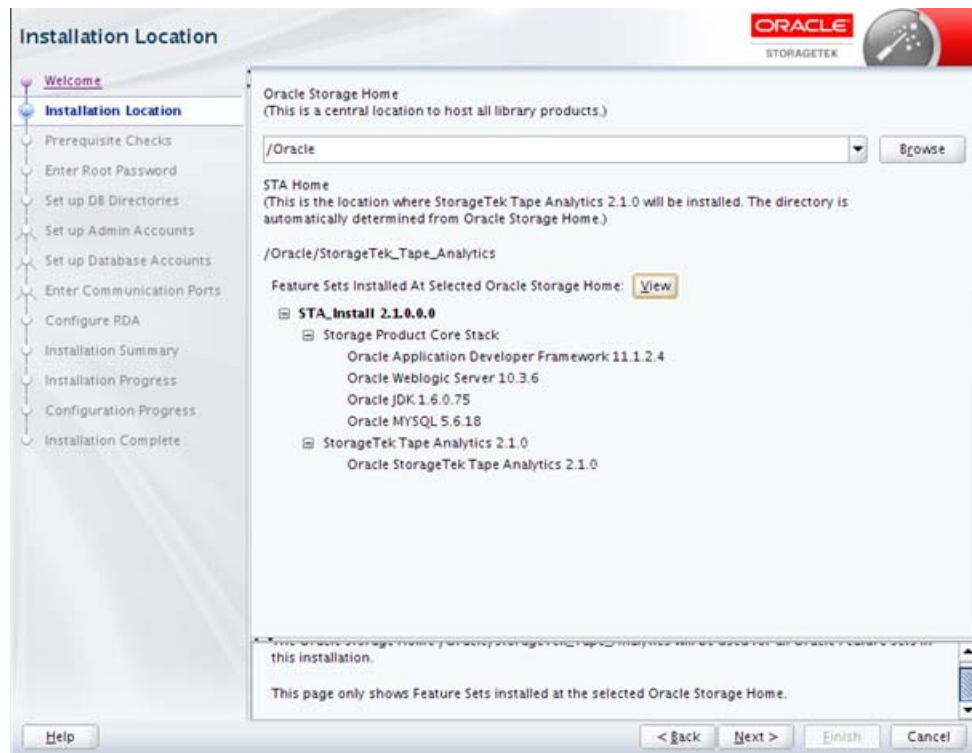
Browse

Click to navigate to the directory you want to specify.

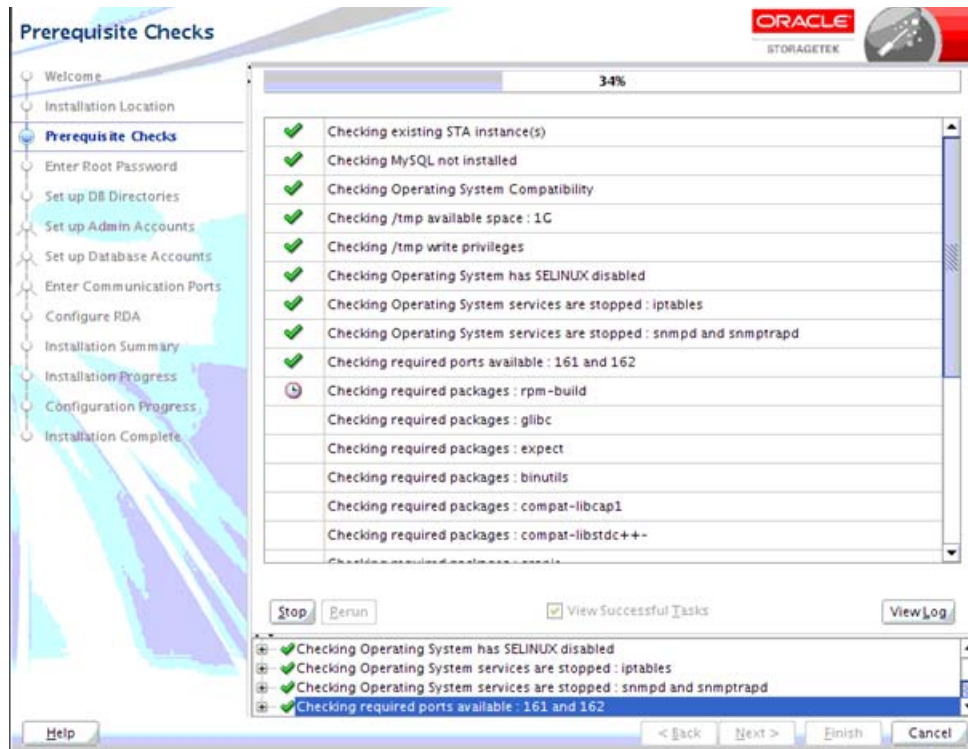
View

Click to display a list of all software currently installed in the Oracle Storage Home directory you have specified. For new installations this list is blank. [Figure A-1](#) is an example of the display after STA has been installed.

Figure A-1 Sample Listing of Oracle Storage Home



Prerequisite Checks



The installer performs a series of tasks to verify that the server environment meets all required and recommended prerequisites. This process may take several minutes.

The possible outcomes of each verification task are as follows:

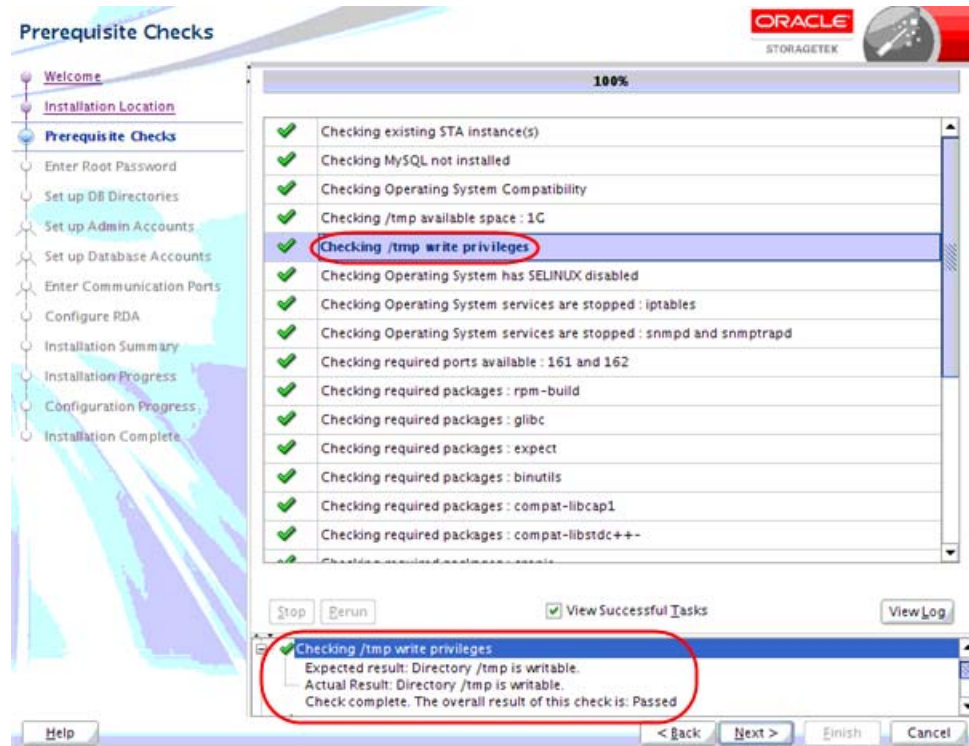
- Success —The prerequisite passed successfully.
- Warning —The recommended prerequisite did not pass.
- Failure —The required prerequisite did not pass.

You cannot continue the installation if there are any Failure outcomes. Additionally, it is recommended that you resolve all Warning outcomes before continuing. You can keep the installer up at this screen while you resolve any issues, and then return and 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. You can use either of the following methods to display expanded detail to help you troubleshoot issues and determine what action to take:

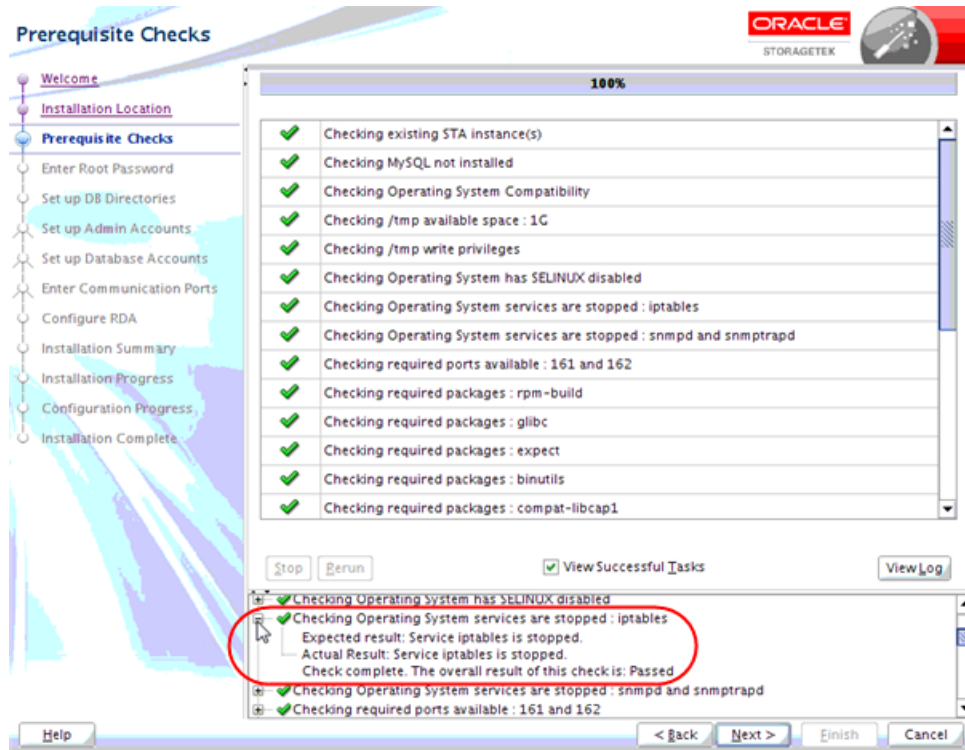
- Select the task in the main window. The task is highlighted in the Message pane with expanded detail. [Figure A-2](#) is an example.

Figure A-2 Task Detail Displayed by Selecting the Task in the Main Window



- In the Message pane, click the **Expand (+)** icon next to the task for which you want to display detail. [Figure A-3](#) is an example. Click the **Collapse (-)** icon to hide the detail again.

Figure A-3 Task Detail Displayed by Selecting the Expand Icon



Screen Fields

None

Screen-specific Buttons

Stop

Click to stop the verification process at the current task. You may want to do this so you can display detail for a selected task that has already completed.

Rerun

Click to run the verification process again from the beginning. This allows you to resolve any Failure or Warning outcomes without exiting and restarting the STA installer.

View Successful Tasks

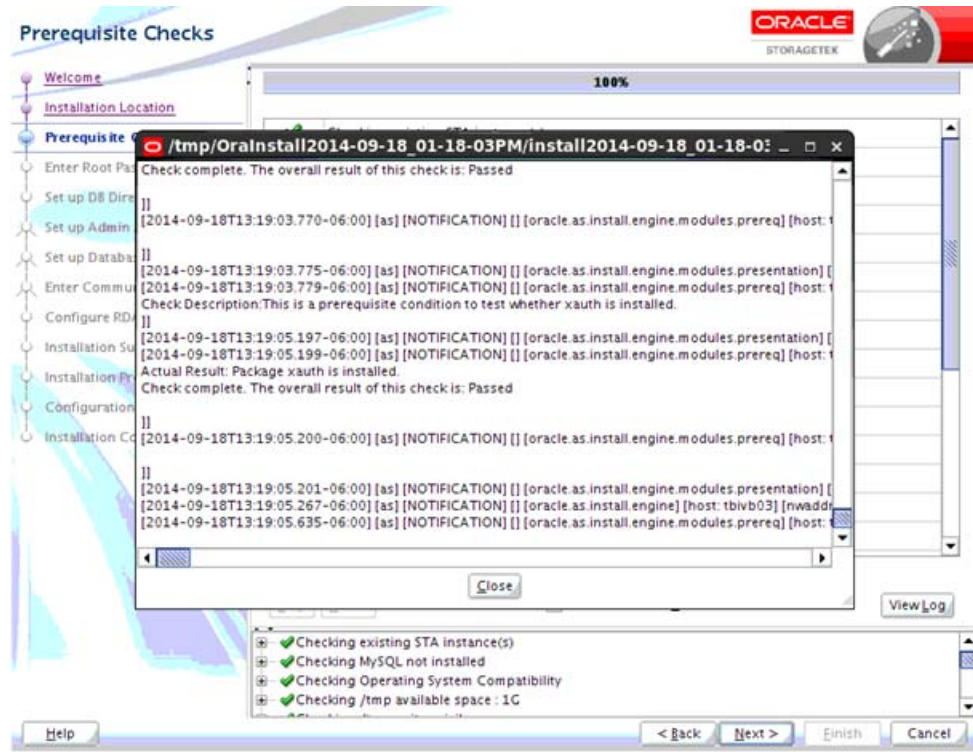
Select the check box to include Success outcomes in the display; this is the default.

Clear the check box to display only Failure or Warning outcomes. This allows you to filter out successful tasks, so you can focus on the ones requiring attention.

View Log

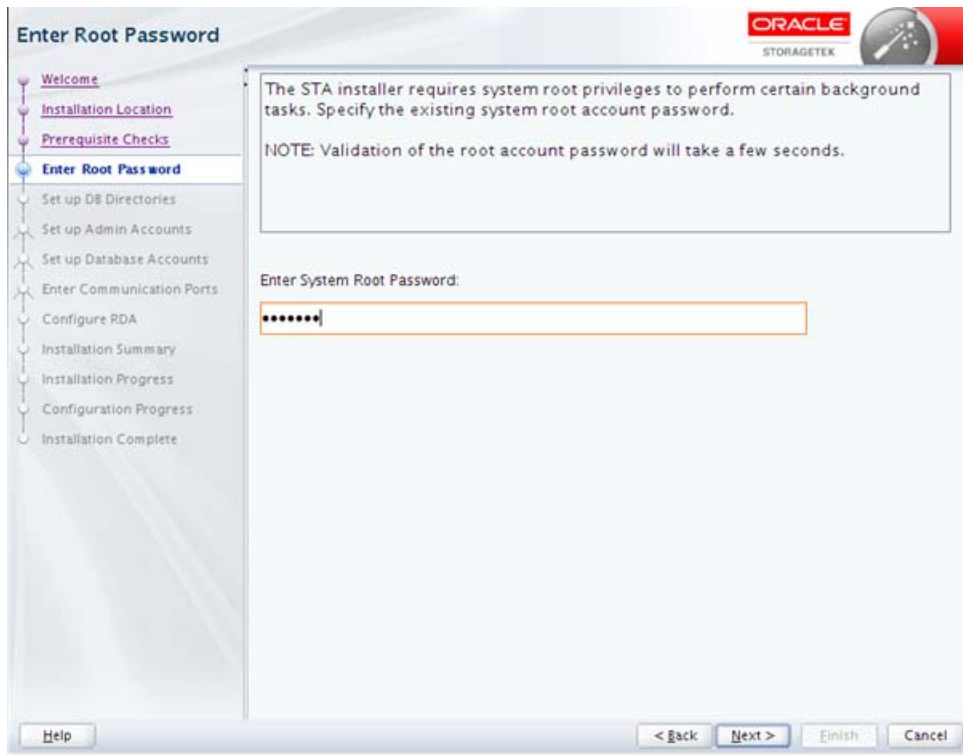
Click to display the prerequisite verification log in a separate window. Figure A-4 is an example. Click **Close** to dismiss the log window.

Figure A-4 Sample Prerequisite Verification Log Display



You can also view the log from the Linux command line. While the installer is running, logs are kept in a subdirectory within /tmp. See ["STA Installation and Deinstallation Logs"](#) on page 3-6 for details.

Enter Root Password



The STA installer requires Linux root access to perform the installation.

Screen Fields

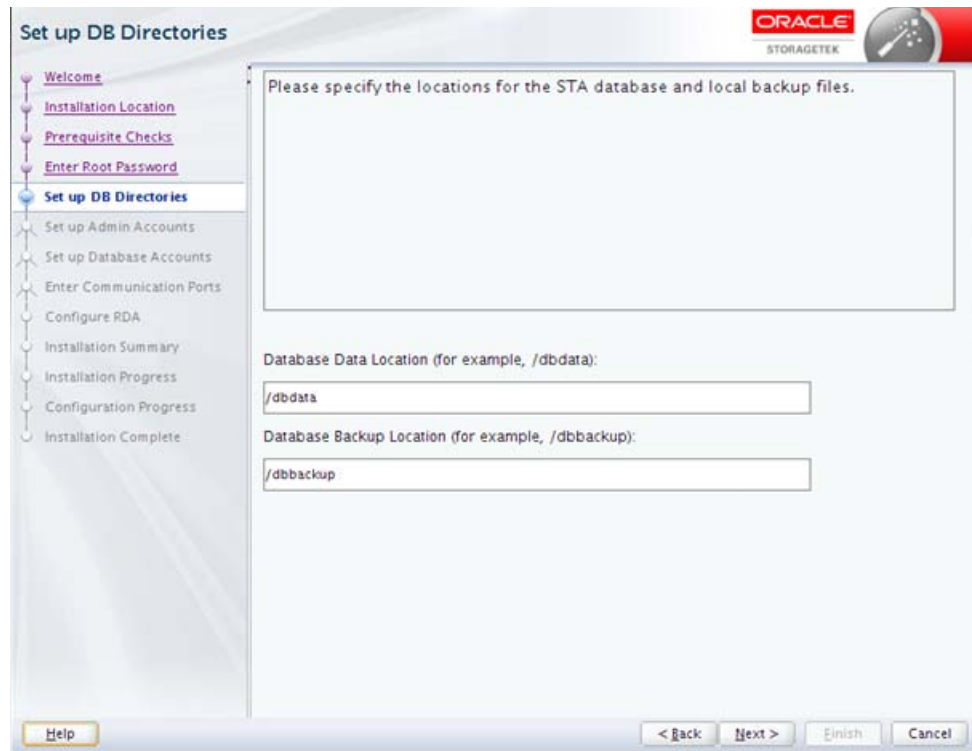
Enter Root Password

Type the password for the system root user. The entry is masked as you type. It may take several seconds to validate the password.

Screen-specific Buttons

None

Set Up DB Directories



This screen allows you to specify locations for the STA database and local STA database backups. The STA installer will create these directories if they do not already exist.

See [Table 2–1, "Recommended File System Layout"](#) for recommendations about these locations.

See the *STA Administration Guide* for information on managing the database services and backups.

Screen Fields

Database Data Location

Required field. Enter the directory where the STA database will be located. This directory cannot be the same as the **Database Backup Location**. You must specify an absolute path.

If the directory you specify already contains a database subdirectory (`mysql`), a warning message is displayed. You can either specify a different database location or accept the current entry, in which case the database subdirectory will be removed during the STA installation.

Database Backup Location

Required field. Enter the directory where STA database backups will be located on the server. This directory cannot be the same as the **Database Data Location**. You must specify an absolute path.

If the directory you specify already contains a database backup subdirectory (`local`), a warning message is displayed. You can either specify a different backup location or accept the current entry, in which case the backup subdirectory will be removed during the STA installation.

Screen-specific Buttons

None

Set Up Admin Accounts



This screen describes the types of information you will define on the next two screens. Read the text, then click **Next** to continue.

Screen Fields

None

Screen-specific Buttons

None

WebLogic Administrator



WebLogic is the application server that hosts STA. You use the WebLogic Administrator account to log into the WebLogic administration console to configure and manage the WebLogic server. This account is used infrequently.

The account will be created during the installation with the credentials you specify.

Caution: Make a secure record of these account credentials; if you lose them, you will not be able to log into the WebLogic administration console and STA must be re-installed.

To protect your site security, usernames and passwords are purposely not preconfigured nor hard-coded.

Screen Fields

See "[Username and Password Requirements](#)" on page 3-3 for detailed requirements.

Enter Username

Type the name you want to assign to the WebLogic Administrator account.

Enter Password

Type the password you want to assign to this account. The entry is masked as you type.

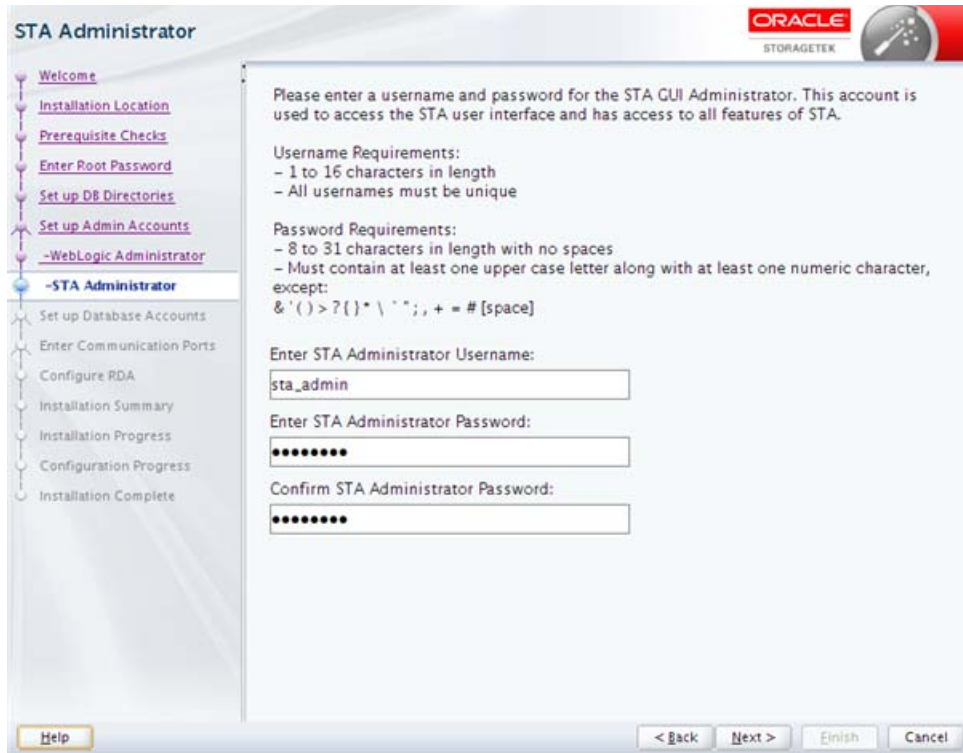
Confirm Password

Type the password again to ensure you have entered it correctly.

Screen-specific Buttons

None

STA Administrator



You use the STA Administrator account to log into the STA user interface. This user has administrator privileges for the STA application and therefore access to all STA screens.

The account will be created during the installation with the credentials you specify.

Caution: Make a secure record of these account credentials; if you lose them, you will not be able to log into the STA user interface.

To protect your site security, usernames and passwords are purposely not preconfigured nor hard-coded.

Screen Fields

See "[Username and Password Requirements](#)" on page 3-3 for detailed requirements.

Enter Username

Type the name you want to assign to the WebLogic Administrator account.

Enter Password

Type the password you want to assign to this account. The entry is masked as you type.

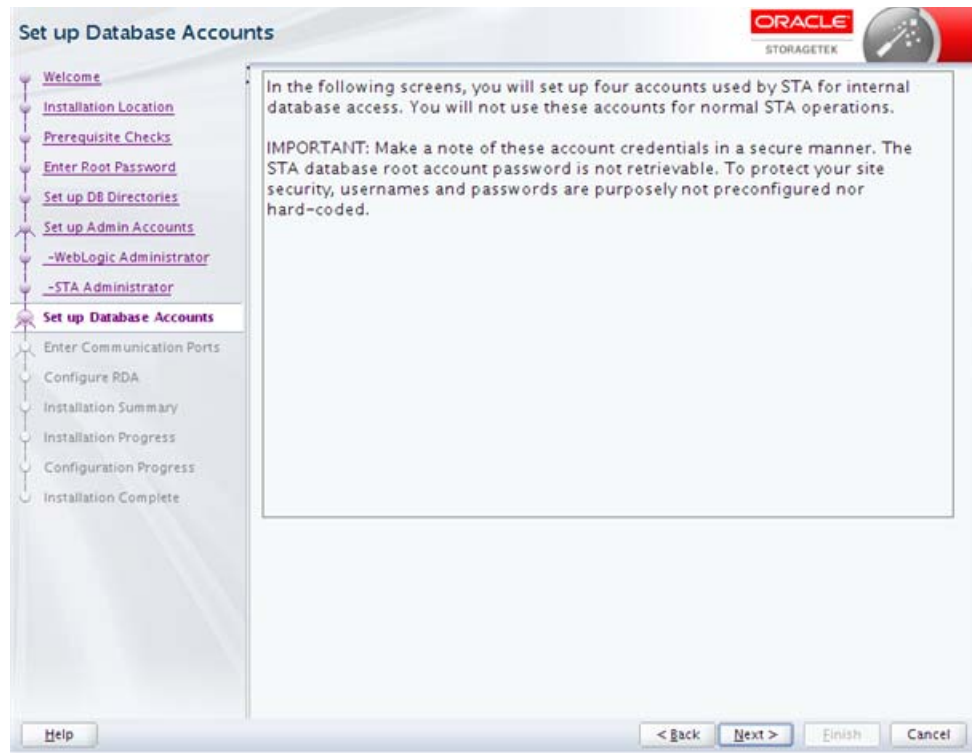
Confirm Password

Type the password again to ensure you have entered it correctly.

Screen-specific Buttons

None

Set Up Database Accounts



This screen describes the types of information you will define on the next four screens. Read the text, then click **Next** to continue.

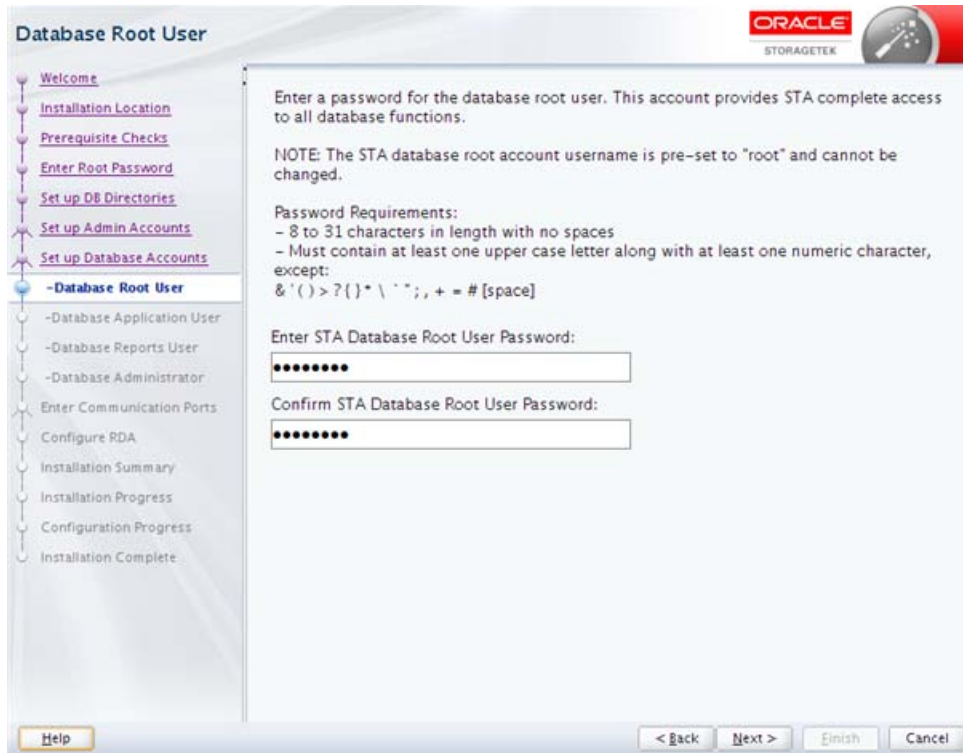
Screen Fields

None

Screen-specific Buttons

None

Database Root User



The STA database root user owns the STA database. This account is used internally by the STA application to create the database, and it provides full access to all database tables. You will not use this account for normal STA operations.

The username for this account is automatically set to `root` and cannot be changed. This is a MySQL account and is separate from the system root user. This account will be created during the installation with the credentials you specify.

Note: Make a secure record of these account credentials.

To protect your site security, usernames and passwords are purposely not preconfigured nor hard-coded.

Screen Fields

See "[Username and Password Requirements](#)" on page 3-3 for detailed requirements.

Enter Username

Type the name you want to assign to the WebLogic Administrator account.

Enter Password

Type the password you want to assign to this account. The entry is masked as you type.

Confirm Password

Type the password again to ensure you have entered it correctly.

Screen-specific Buttons

None

Database Application User

The database application account is a MySQL account used internally by the STA application to connect to and update the STA database. The account provides create, update, delete, and read access to all database tables. You will not use this account for normal STA operations.

This account will be created during the installation with the credentials you specify.

Note: Make a secure record of these account credentials.

To protect your site security, usernames and passwords are purposely not preconfigured nor hard-coded.

Screen Fields

See "[Username and Password Requirements](#)" on page 3-3 for detailed requirements.

Enter Username

Type the name you want to assign to the WebLogic Administrator account.

Enter Password

Type the password you want to assign to this account. The entry is masked as you type.

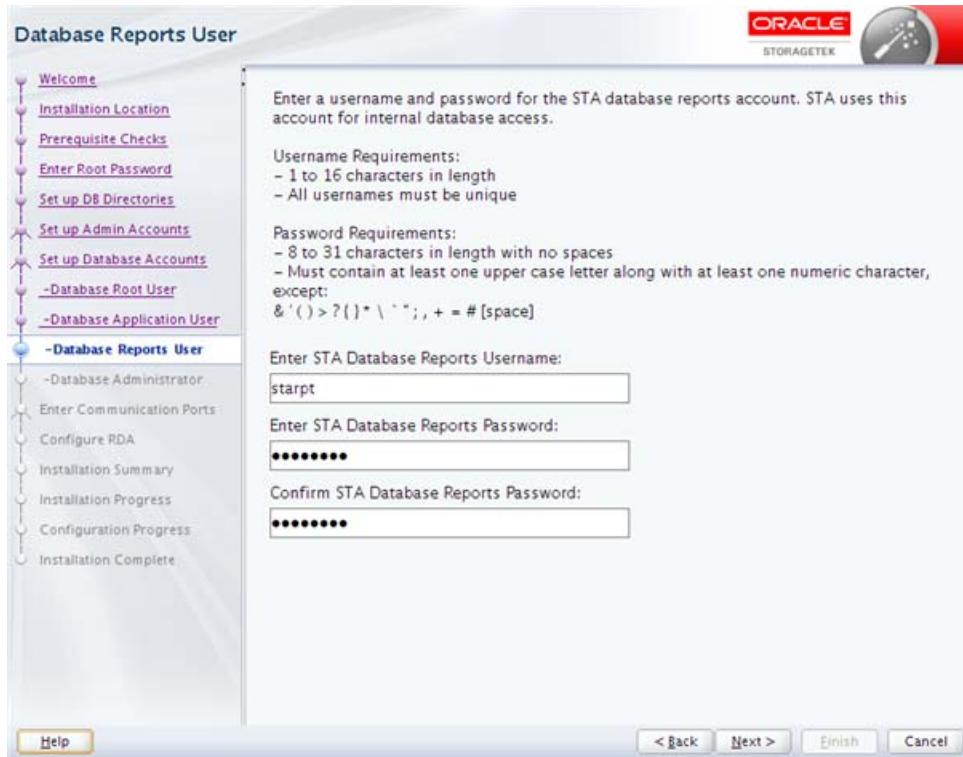
Confirm Password

Type the password again to ensure you have entered it correctly.

Screen-specific Buttons

None

Database Reports User



The STA database reports account is a MySQL account used by non-STA and third-party applications to connect to the STA database. The account provides read-only access to selected database tables. You will not use this account for normal STA operations.

This account will be created during the installation with the credentials you specify.

Note: Make a secure record of these account credentials.

To protect your site security, usernames and passwords are purposely not preconfigured nor hard-coded.

Screen Fields

See "[Username and Password Requirements](#)" on page 3-3 for detailed requirements.

Enter Username

Type the name you want to assign to the WebLogic Administrator account.

Enter Password

Type the password you want to assign to this account. The entry is masked as you type.

Confirm Password

Type the password again to ensure you have entered it correctly.

Screen-specific Buttons

None

Database Administrator

The STA database administrator account is a MySQL account used internally by STA administration and monitoring utilities to connect to the STA database and configure and run scheduled backups. The account provides full access, except the "grant" option, to all database tables. You will not use this account for normal STA operations.

This account will be created during the installation with the credentials you specify.

Note: Make a secure record of these account credentials.

To protect your site security, usernames and passwords are purposely not preconfigured nor hard-coded.

Screen Fields

See "[Username and Password Requirements](#)" on page 3-3 for detailed requirements.

Enter Username

Type the name you want to assign to the WebLogic Administrator account.

Enter Password

Type the password you want to assign to this account. The entry is masked as you type.

Confirm Password

Type the password again to ensure you have entered it correctly.

Screen-specific Buttons

None

Enter Communication Ports



This screen describes the types of information you will define on the next four screens. Read the text, then click **Next** to continue.

You will provide values for the configurable internal and external WebLogic and STA ports. The ports will be configured and enabled during the installation with the values you specify. The port numbers you specify must be unique, and the ports must remain available and dedicated to STA.

Note: Before completing these screens, verify the correct port number values with your network administrator. Once STA has been installed, the port numbers cannot be changed without deinstalling and reinstalling STA.

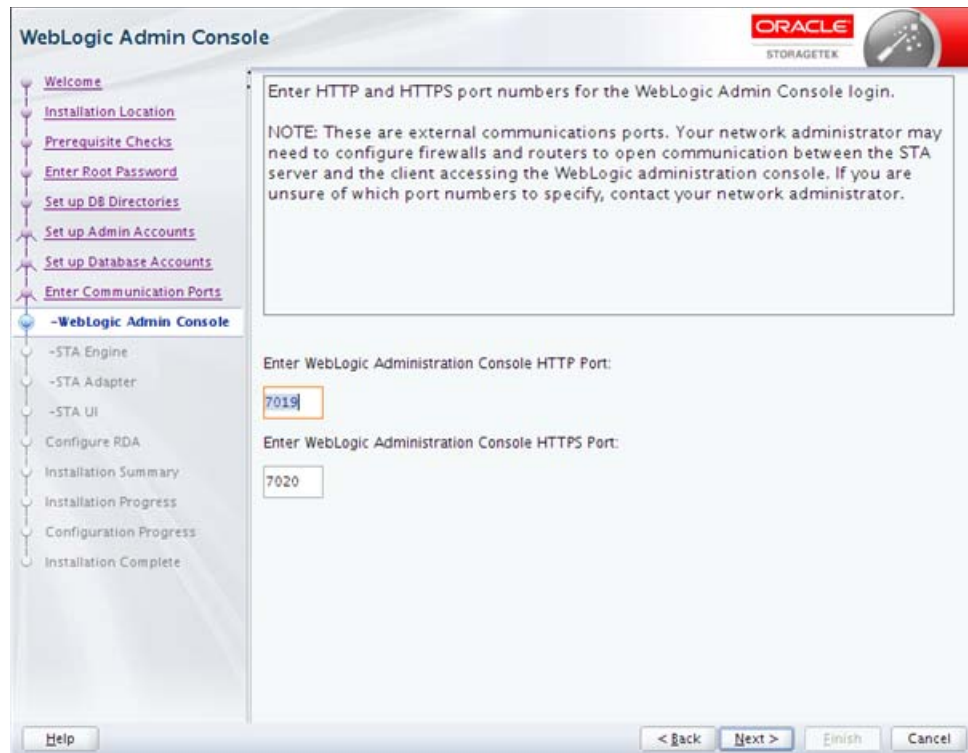
Screen Fields

None

Screen-specific Buttons

None

WebLogic Admin Console



You specify the WebLogic Administrator console port number when you log into the WebLogic Administrator console, which is used to administer and configure the WebLogic application server.

Note: These are external communication ports. Your network administrator may need to configure firewalls and routers to open communication between the STA server and the client accessing the WebLogic Administration console.

Note: Make a secure record of these port numbers; they cannot be changed once STA is installed.

To protect your site security, these numbers are purposely not preconfigured nor hard-coded.

Screen Fields

Enter HTTP Port

Enter the HTTP port number for unsecure access to the WebLogic Administrator console login. Typically this port number is 7019.

Port numbers must be unique and available.

Enter HTTPS Port

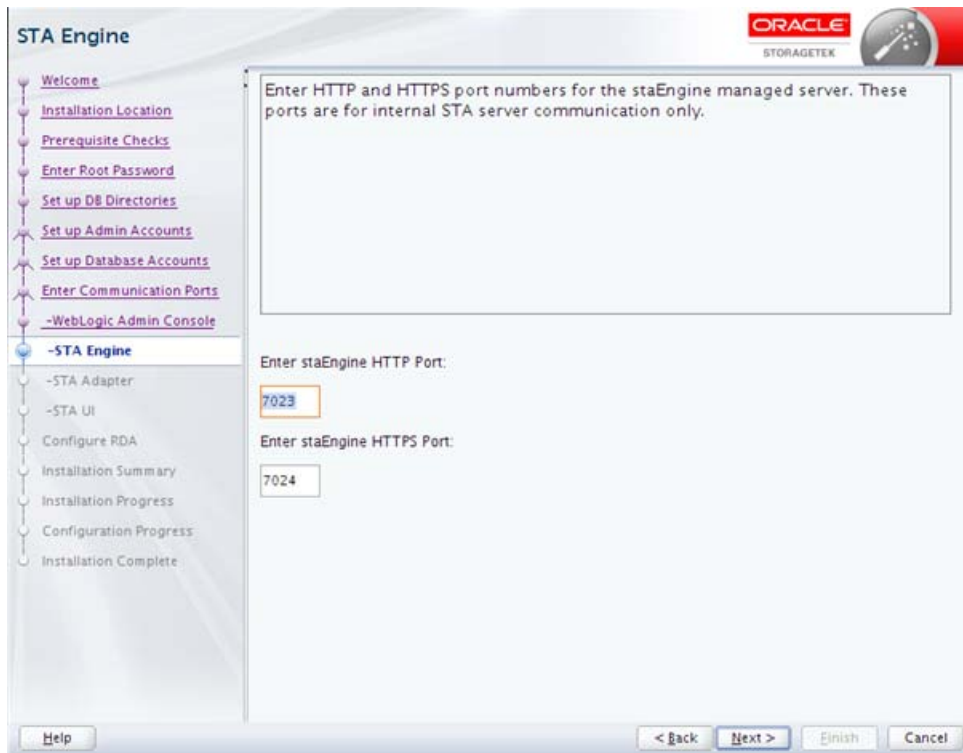
Enter the HTTPS port number for secure access to the WebLogic Administrator console login. Typically this port number is 7020.

Port numbers must be unique and available.

Screen-specific Buttons

None

STA Engine



The staEngine managed server ports are used for internal STA server communication only.

Note: Make a secure record of these port numbers; they cannot be changed once STA is installed.

To protect your site security, these numbers are purposely not preconfigured nor hard-coded.

Screen Fields

Enter HTTP Port

Enter the HTTP port number for unsecure access to the staEngine managed server. Typically this port number is 7023.

Port numbers must be unique and available.

Enter HTTPS Port

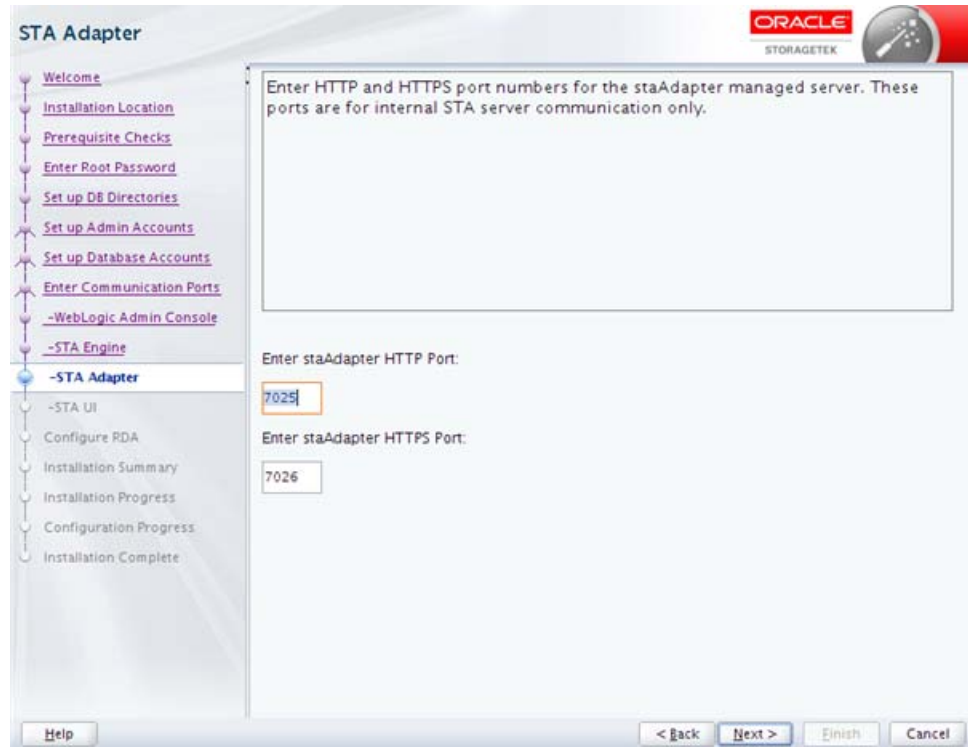
Enter the HTTPS port number for secure access to the staEngine managed server. Typically this port number is 7024.

Port numbers must be unique and available.

Screen-specific Buttons

None

STA Adapter



The staAdapter managed server ports are used for internal SNMP communication only.

Note: Make a secure record of these port numbers; they cannot be changed once STA is installed.

To protect your site security, these numbers are purposely not preconfigured nor hard-coded.

Screen Fields

Enter HTTP Port

Enter the HTTP port number for unsecure access to the staAdapter managed server. Typically this port number is 7025.

Port numbers must be unique and available.

Enter HTTPS Port

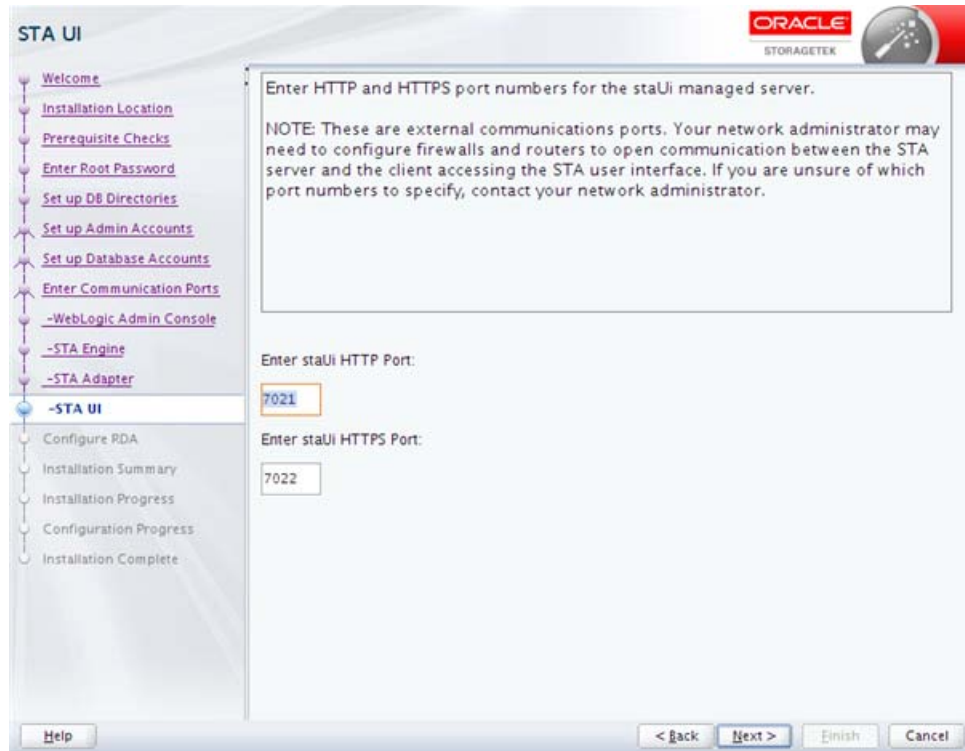
Enter the HTTPS port number for secure access to the staAdapter managed server. Typically this port number is 7026.

Port numbers must be unique and available.

Screen-specific Buttons

None

STA UI



You specify the staUi managed server port number when you log into the STA application user interface.

Note: These are external communication ports. Your network administrator may need to configure firewalls and routers to open communication between the STA server and the client accessing the WebLogic Administration console.

Note: Make a secure record of these port numbers; they cannot be changed once STA is installed.

To protect your site security, these numbers are purposely not preconfigured nor hard-coded.

Screen Fields

Enter HTTP Port

Enter the HTTP port number for unsecure access to the staUi managed server. Typically this port number is 7021.

Port numbers must be unique and available.

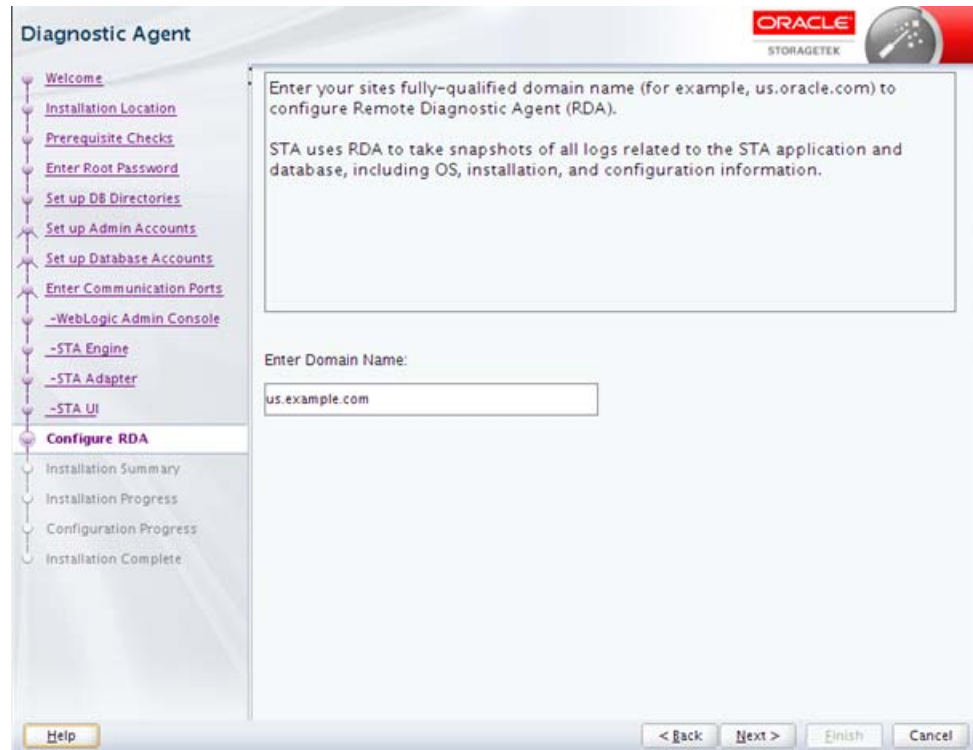
Enter HTTPS Port

Enter the HTTP port number for secure access to the staUi managed server. Typically this port number is 7022.

Port numbers must be unique and available.

Screen-specific Buttons

None

Diagnostic Agent

The STA installer uses your site's fully qualified domain name to configure Oracle's Remote Diagnostic Agent (RDA).

STA uses RDA to take snapshots of all logs related to the STA application and database, including operating system, installation, and configuration information. See the *STA User's Guide* for additional information.

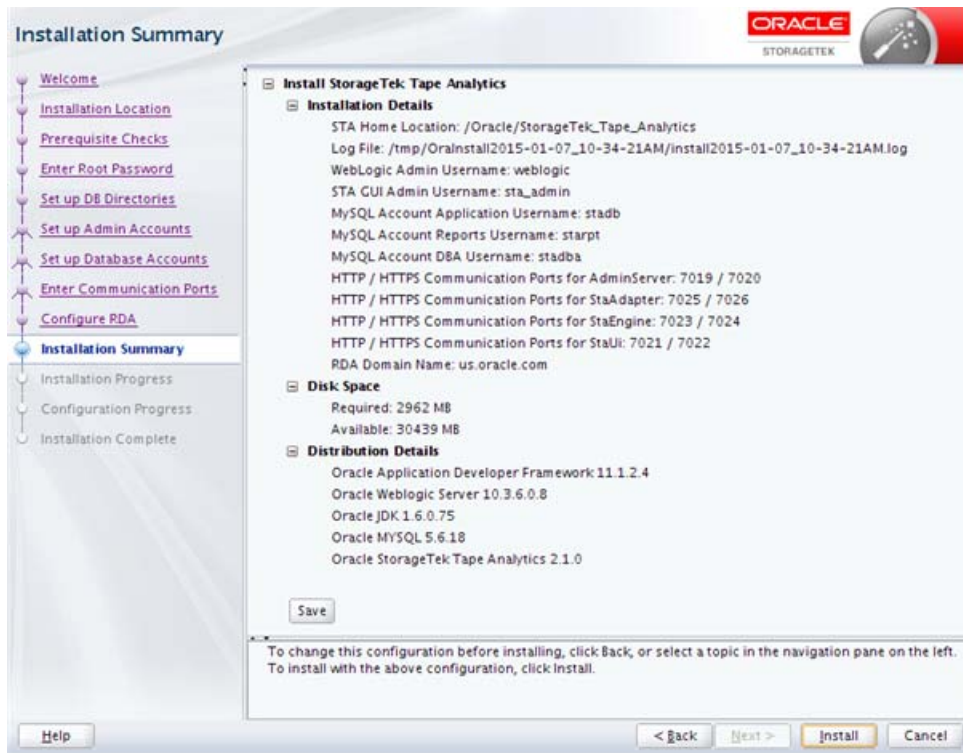
Screen Fields**Enter Domain Name**

Enter your site's fully qualified domain name; for example, us.example.com.

Screen-specific Buttons

None

Installation Summary



The screen displays the following details about the installation. You can save this information to a text file for your records.

- Installation Details—Information you have entered on the installer screens.
- Disk Space—Required and available disk space, in MB.
- Distribution Details—Names and version numbers of the software packages that will be installed.

Continue as follows:

- To change any of the Installation Details, click **Back** to return to the applicable screen, or select the screen link in the navigation pane to go directly to the screen.
- To save the displayed details in a text file, click **Save**.
- To install using the displayed values, click **Install**.
- To cancel the installation, click **Cancel**.

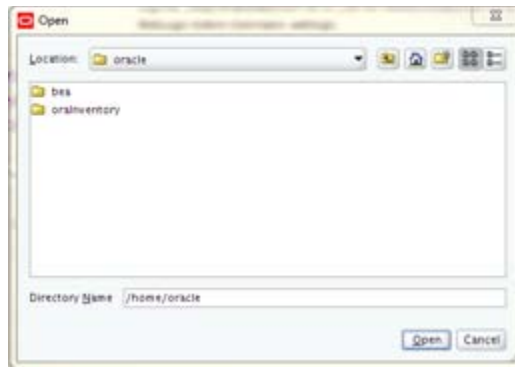
Screen Fields

None

Screen-specific Buttons

Save

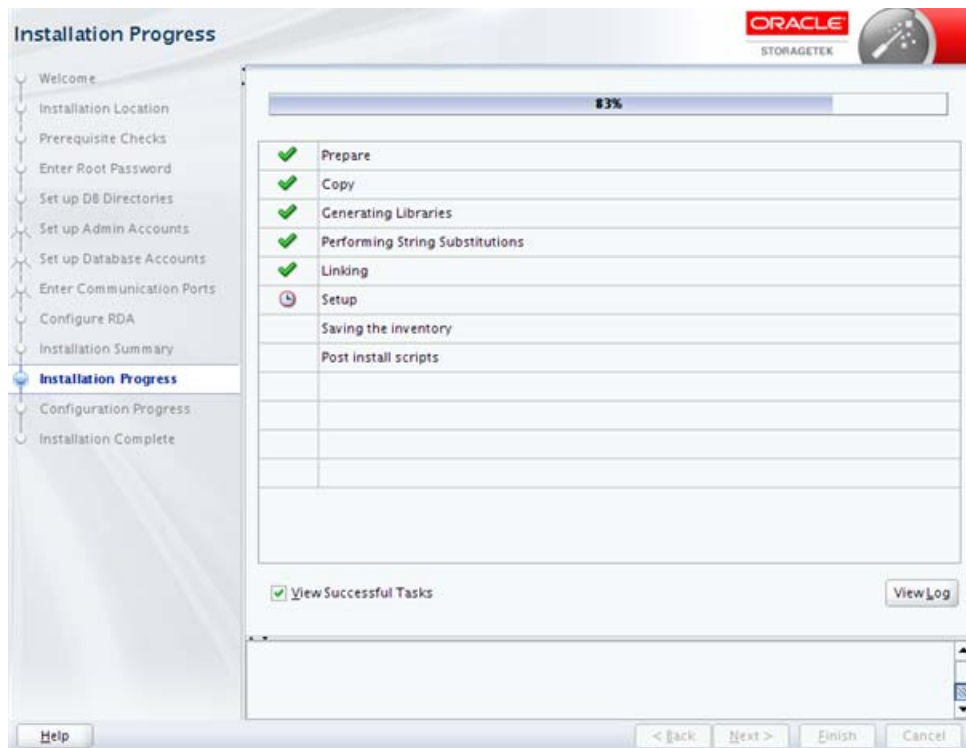
Click to save the displayed information to a text file with the name `STA_Installation_Profile_timestamp.txt`. In the Open dialog box, specify the directory where you want the file to be saved.



Install

Click to begin the installation. Once you click this button, you cannot pause or cancel the installation.

Installation Progress



The STA installation begins and the screen displays the status of each task.

Caution: Do not close this window or otherwise interrupt the installation while it is in progress, as this may leave incomplete installation components on the server.

If a task fails, the installation stops and you must exit the installer by clicking **Cancel**. The installer will roll back the installation and return the server to its original state.

Before you exit, you can view additional detail in the Message pane to help you troubleshoot issues and determine what action to take. You can also view the installation log for additional information.

Screen Fields

None

Screen-specific Buttons

View Successful Tasks

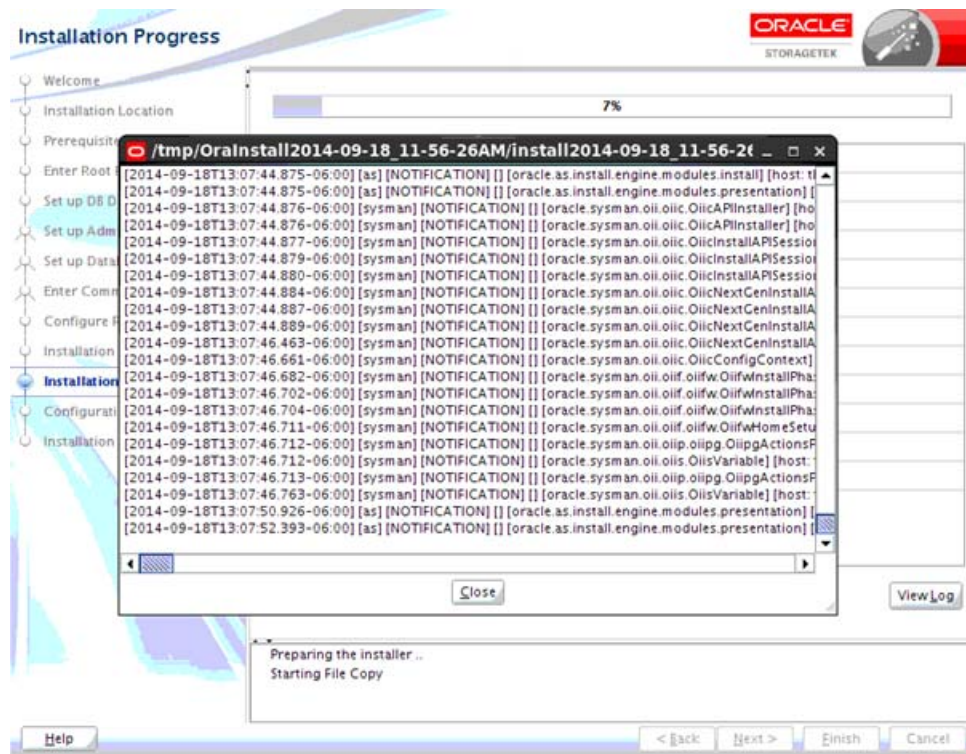
Select the check box to include Success outcomes in the display; this is the default.

Clear the check box to display only Failure outcomes. This allows you to filter out successful tasks, so you can focus on the ones requiring attention.

View Log

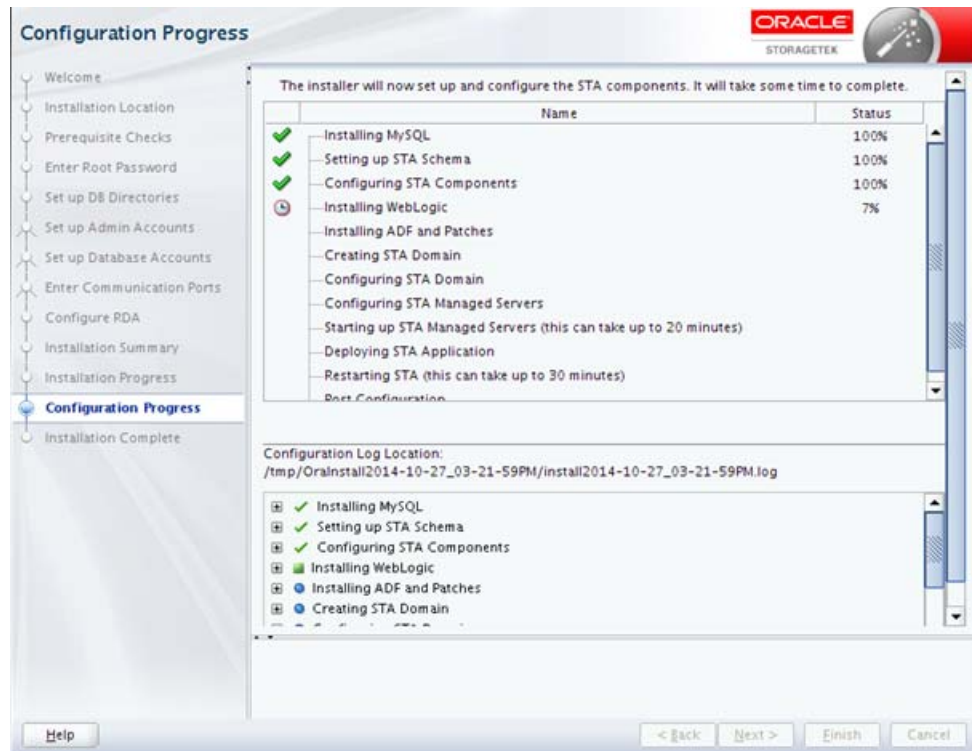
Click to display the installation log in a separate window. [Figure A-5](#) is an example. Click **Close** to dismiss the log window.

Figure A-5 Sample Installation Progress Log Display



You can also view the log from the Linux command line. While the installer is running, logs are kept in a subdirectory within /tmp. See "[STA Installation and Deinstallation Logs](#)" on page 3-6 for details.

Configuration Progress



The STA configuration and deployment begins, and the screen displays the status of each task.

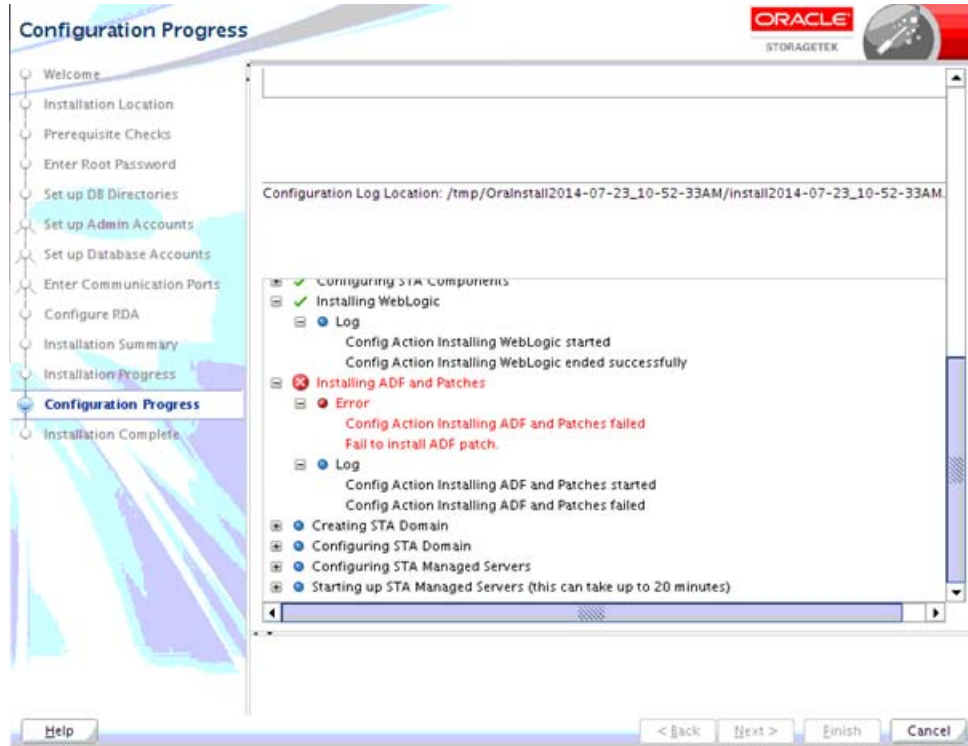
Caution: Do not close this window or otherwise interrupt the configuration while it is in progress, as this may leave incomplete installation components on the server.

During this process, the WebLogic server, STA managed servers, and the STA application are configured and started. This may take 30 to 60 minutes to complete.

You can display expanded detail for any completed or in-progress task. In the Message pane, click the **Expand** (+) icon next to the task for which you want to display detail. Click the **Collapse** (–) icon to hide the detail again. [Figure A-6](#) is an example showing expanded detail for successful and unsuccessful tasks.

If a task fails, the STA installer quits, rolls back the installation, and returns the server to its original state. You can view the installation log to troubleshoot the issue. See ["STA Installation and Deinstallation Logs"](#) on page 3-6 for details.

Figure A-6 Sample Configuration Progress Detail



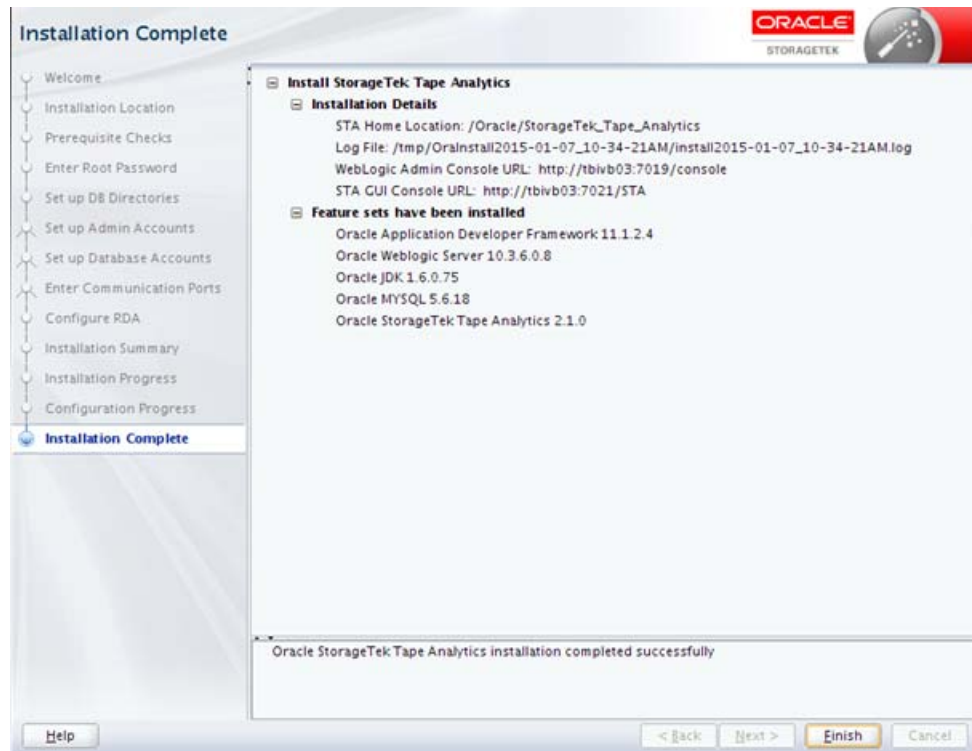
Screen Fields

None

Screen-specific Buttons

None

Installation Complete



The screen displays the following details about the completed installation:

- Installation Details—Locations of the installed STA application and installer log file, and connection details for the WebLogic and STA application user interfaces.
- Feature sets have been installed—Names and version numbers of the software packages that have been installed.

You may wish to save a screen shot of this information for your records. Click **Finish** to exit the installer.

Screen Fields

None

Screen-specific Buttons

Finish

Click to exit the STA installer.

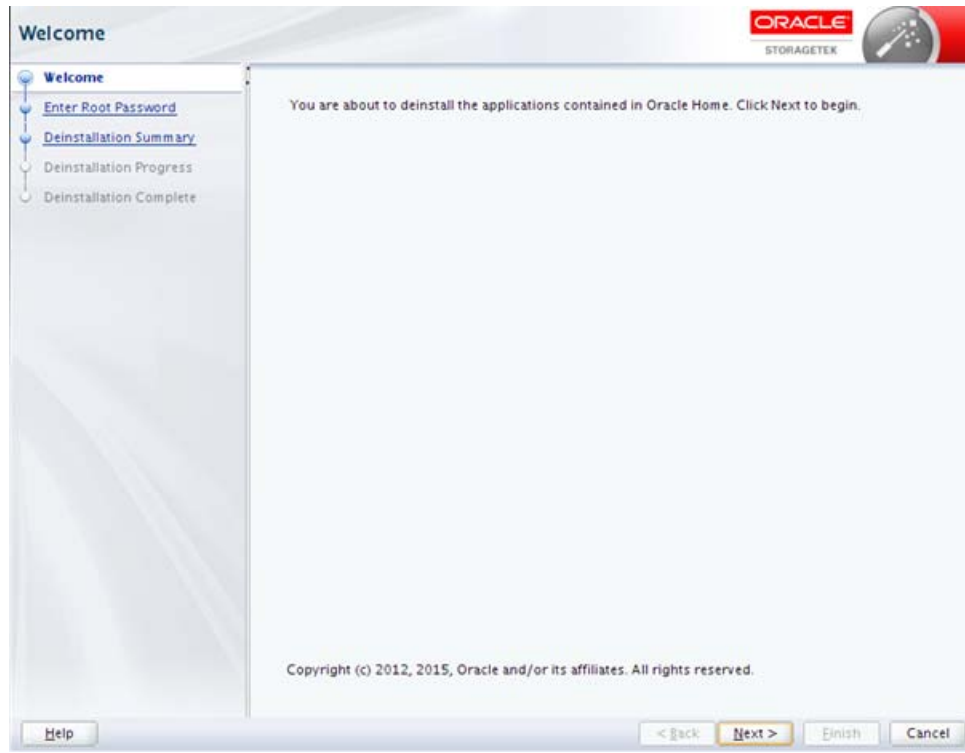
STA Graphical Deinstaller Screens

This section provides detailed reference for each screen of the STA graphical deinstaller.

- "Welcome" on page A-36
- "Enter Root Password" on page A-37
- "Deinstallation Summary" on page A-38
- "Deinstallation Progress" on page A-39

- "Deinstallation Complete" on page A-41

Welcome



The screen confirms that you are about to deinstall the STA application and all associated software, including WebLogic Server and MySQL. Read the text and click **Next** to proceed.

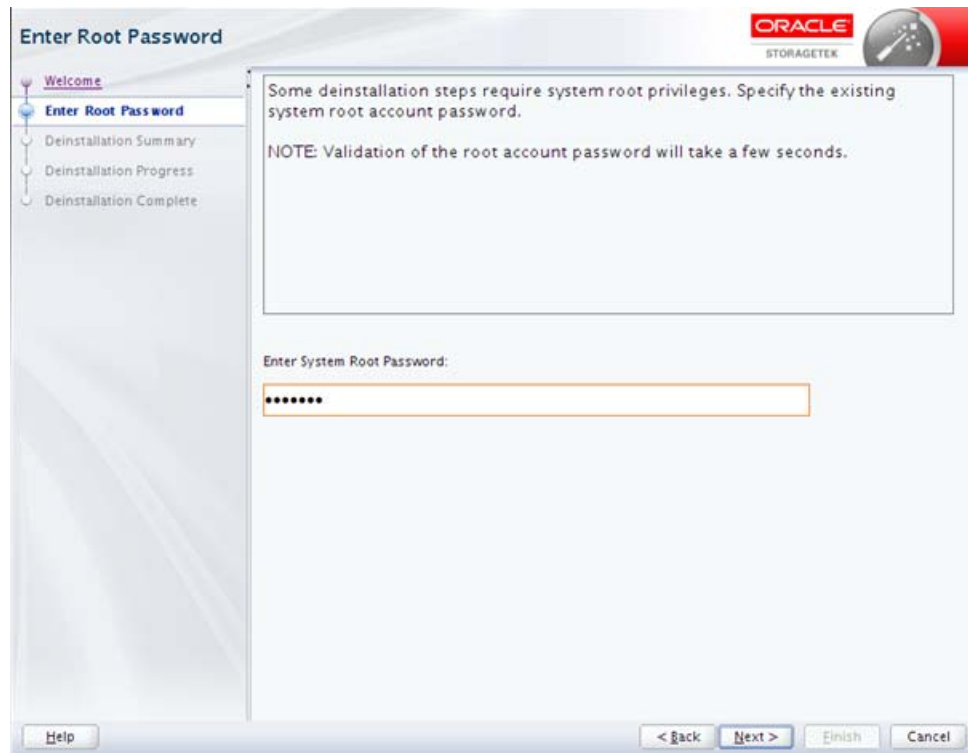
Screen Fields

None

Screen-specific Buttons

None

Enter Root Password



The STA deinstaller requires Linux root access to perform the deinstallation tasks.

Screen Fields

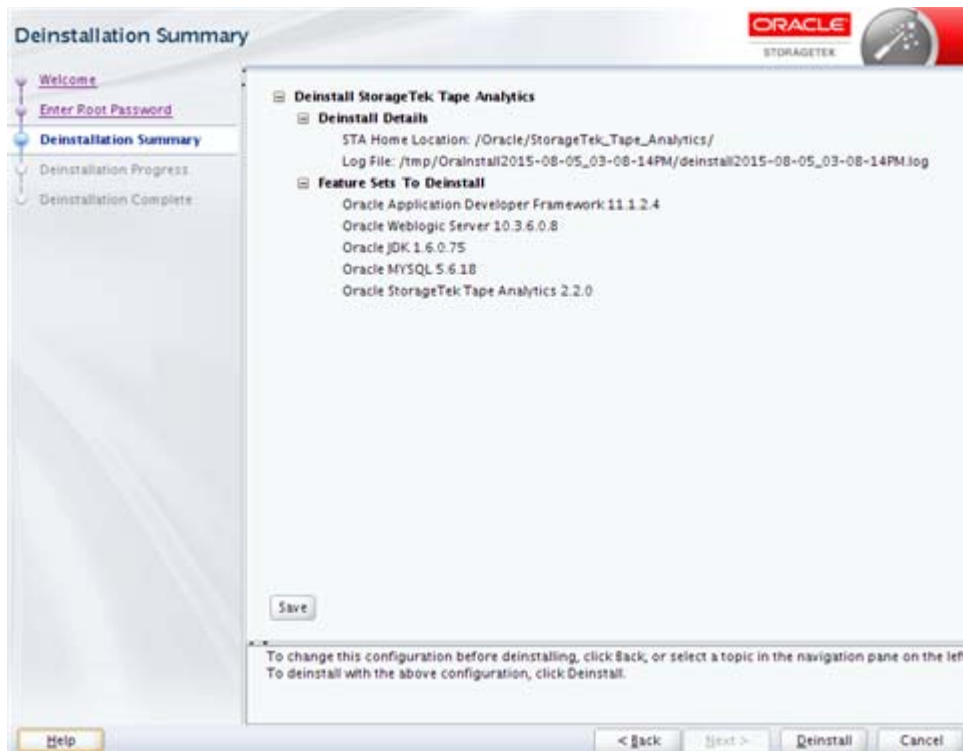
Enter Root Password

Type the password for the system root user. The entry is masked as you type. It may take several seconds to validate the password.

Screen-specific Buttons

None

Deinstallation Summary



The screen displays the following details about the software that will be deinstalled:

- Deinstall Details—Locations of the STA application software and the deinstallation log.
- Feature Sets to Deinstall—Names and version numbers of the software packages that will be deinstalled.

Verify this information, and then continue as follows:

- Click **Cancel** to cancel and exit the deinstaller.
- Click **Deinstall** to proceed with the deinstallation.

Screen Fields

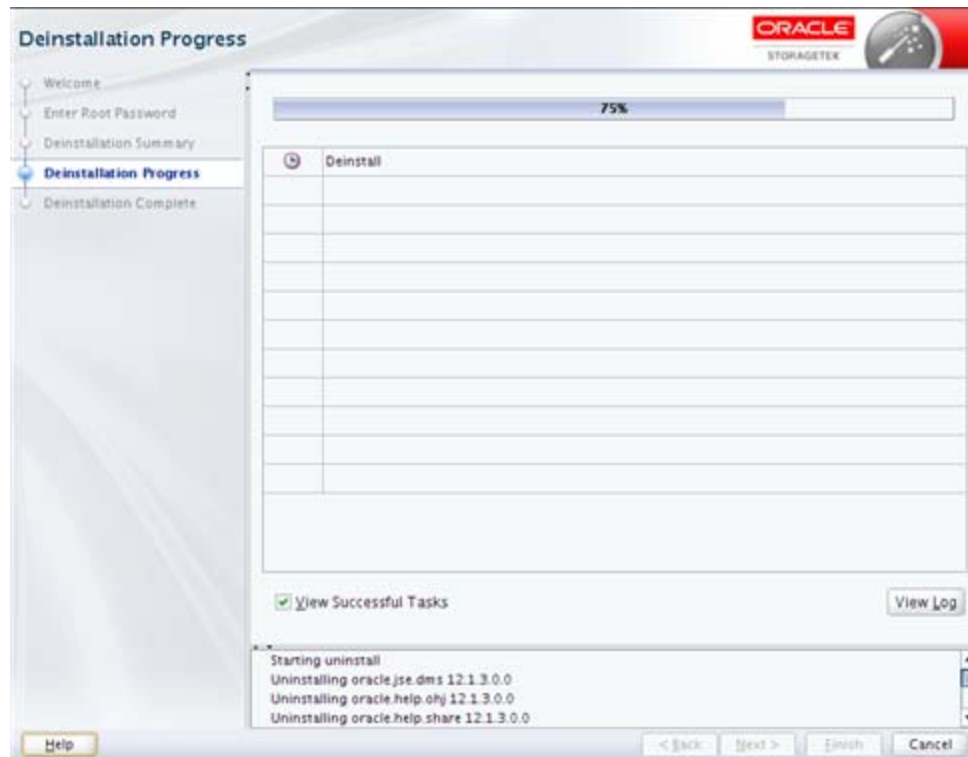
None

Screen-specific Buttons

Deinstall

Click to begin deinstalling STA. Once you click this button, you cannot pause or cancel the deinstallation.

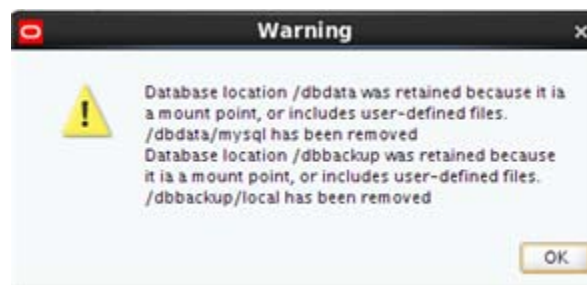
Deinstallation Progress



The STA deinstallation begins, and the screen displays the status of each task.

Caution: Do not close this window or otherwise interrupt the deinstallation while it is in progress, as this may leave incomplete STA components on the server.

Note: 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.



When the deinstallation completes, the message "Deinstallation Successful" appears in the Message pane. Click **Next** or **Finish** to proceed to the final screen.

If a task fails, the STA deinstaller quits, rolls back the deinstallation, and returns the server to its original state. You can view the deinstallation log to troubleshoot the issue. See ["STA Installation and Deinstallation Logs"](#) on page 3-6 for details.

Screen Fields

None

Screen-specific Buttons

View Successful Tasks

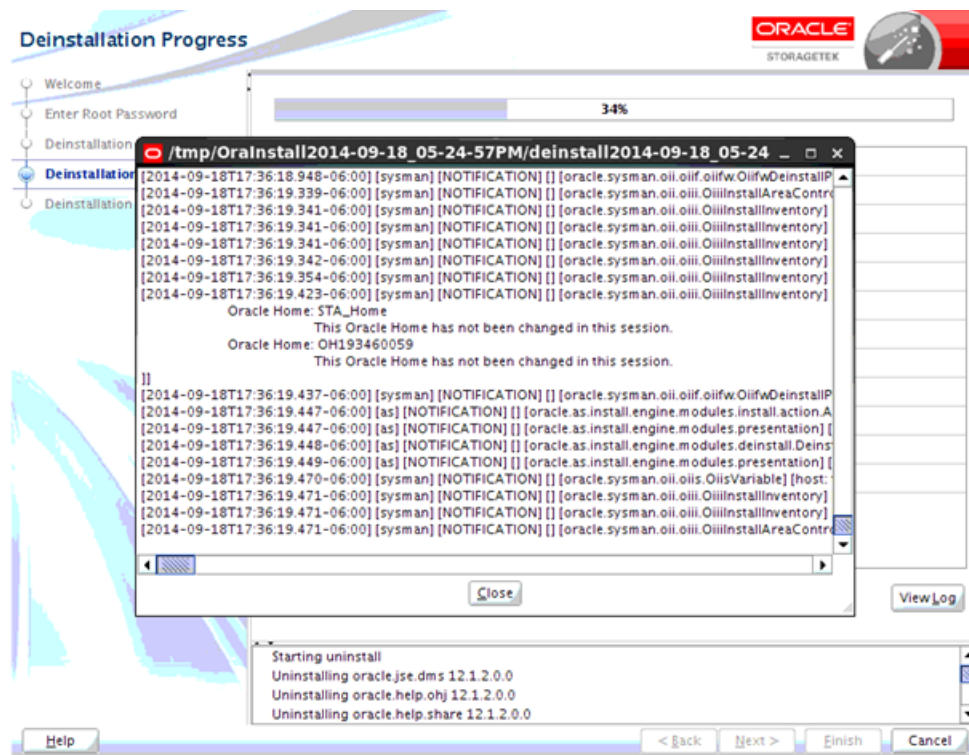
Select the check box to include Success outcomes in the display; this is the default.

Clear the check box to display only Failure outcomes. This allows you to filter out successful tasks, so you can focus on the ones requiring attention.

View Log

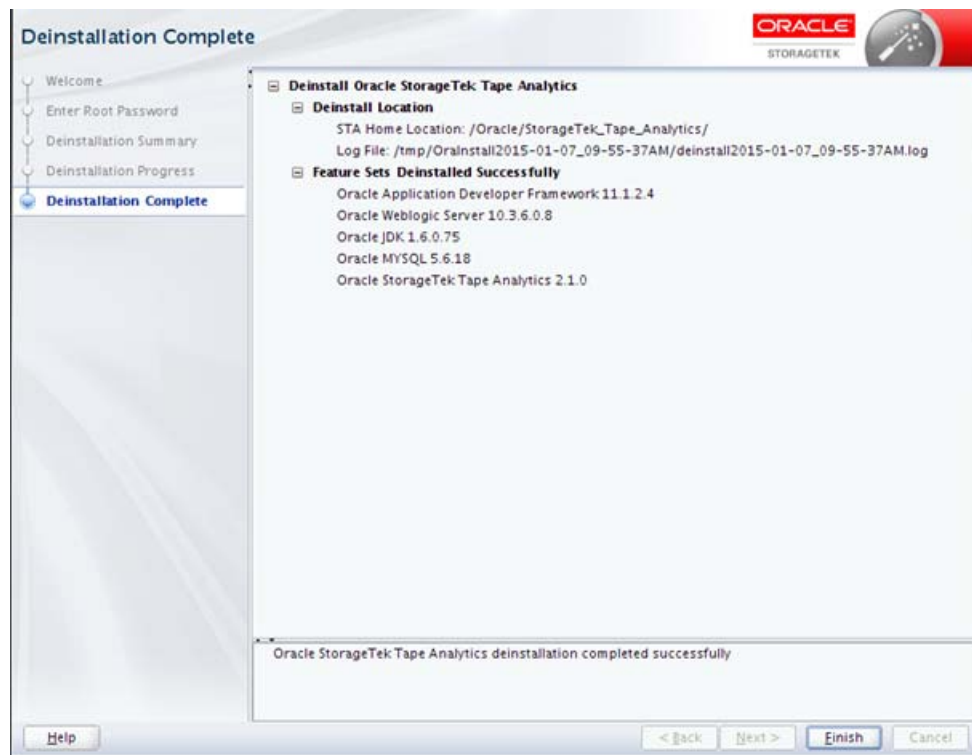
Click to display the deinstallation log in a separate window. [Figure A-7](#) is an example. Click **Close** to dismiss the log window.

Figure A-7 Sample Deinstallation Progress Log Display



You can also view the log from the Linux command line. While the deinstaller is running, logs are kept in a subdirectory within /tmp. See "[STA Installation and Deinstallation Logs](#)" on page 3-6 for details.

Deinstallation Complete



The screen displays the details about the software packages that have been deinstalled.

Screen Fields

None

Screen-specific Buttons

Finish

Click to exit the STA deinstaller.

STA Silent-mode Installer and Deinstaller

This appendix includes the following sections:

- [Using the STA Silent-mode Installer and Deinstaller](#)
- [Silent Mode Tasks](#)
- [Response File Reference Information](#)
- [STA Installer and Deinstaller Command Options](#)

Using the STA Silent-mode Installer and Deinstaller

Silent mode allows you to bypass the graphical user interface and supply the STA installation or deinstallation options in text file called the *response file*.

Silent mode is useful for unattended installation and deinstallation operations, and for ensuring consistent STA installations on multiple machines. By using a response file, you can supply a single set of parameters and automate the installation or deinstallation. You can run silent mode either from a script or from the Linux command line.

Silent Mode Requirements

See "[Verify Installation Prerequisites](#)" on page 3-9 for general STA installation requirements. In addition, the STA silent-mode installer and deinstaller have the following mode-specific requirements:

- 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.
- Before using silent mode, you must download the response file build utility from the Oracle Software Delivery Cloud website and use it to create the response file with encrypted passwords. See "[Response file build utility](#)" on page B-2 for details.
- Silent mode also requires a central inventory pointer file specifying the location of the Oracle central inventory directory and the Oracle install group. You must create the file manually if it does not exist already. See "[Oracle central inventory pointer file](#)" on page B-2 for details.

Files and Utilities Used With Silent Mode

Following are details about the files and utilities used with the silent-mode installer and deinstaller.

Response files

Response files contain all configuration settings necessary for the silent-mode installer or deinstaller to run unattended. They are not used with graphical mode.

You use the response file build utility to create response files with the correct format and parameters. Following are the default response file names created by the utility. You can rename the files after they are created.

- `silentInstall.rsp`—Installer response file
- `silentDeinstall.rsp`—Deinstaller response file

When you run the silent-mode installer or deinstaller, you must use the `-responseFile` parameter to specify the full path to the response file you want to use.

See "[Sample Response Files](#)" on page B-18 for complete sample files with values.

Note: You can use a response file any number of times, but to protect your site security, once a response file has been used for a successful installation or deinstallation, you cannot reuse the file until you reenter the encrypted passwords. See "[Add or Modify Encrypted Passwords in an Existing Response File](#)" on page B-10 for instructions.

Response file build utility

The response file build utility allows you to create a response file with all parameter values and passwords needed for the silent-mode installer or deinstaller. The utility prompts you for the necessary information and saves the response file and an encryption key file to the directory of your choice. It writes passwords to the file in encrypted form.

You can download the response file build utility when you download the STA installer. The utility name is `silentInstallUtility_<version>.jar`, where *version* is the STA version number. See "[Download STA](#)" on page 3-11 for details.

See "[Response File Build Utility Options](#)" on page B-16 for details about the utility.

Oracle central inventory pointer file

The STA silent-mode installer and deinstaller use the Oracle central inventory location and Oracle install group specified in the central inventory pointer file. See "[Users, Groups, and Locations Used by the STA Installer](#)" on page 3-1 for details.

By default, silent mode uses the pointer file `/etc/oralnst.loc`. When you register the Oracle central inventory, the file is automatically created with this name and location. See "[Register the Oracle Central Inventory Location](#)" on page 3-19 for details.

If the Oracle central inventory location has *not* been registered, you must create the pointer file manually and give it the filename `oralnst.loc`. See "[Identify or Create Information Required for the Installation](#)" on page 3-7 for instructions.

You can locate the pointer file in any directory, but if it is not in `/etc`, you must use the `-invPtrLoc` parameter to specify the file location when you run the silent-mode installer or deinstaller. See "[-invPtrLoc pointer_file](#)" on page B-20 for details about this parameter.

Silent Mode Process

Use this process to perform a silent mode installation or deinstallation.

1. Perform the necessary prerequisite activities, as follows:

- For installations, use the following procedures to obtain the necessary information, verify prerequisites, and download the STA installer files and response file build utility.
 - a. ["Identify or Create Information Required for the Installation"](#) on page 3-7
 - b. ["Verify Installation Prerequisites"](#) on page 3-9
 - c. ["Download STA"](#) on page 3-11
 - For deinstallations, download the response file build utility if you have not done so already. See ["Download STA"](#) on page 3-11 for instructions.
2. Use the response file build utility to create a response file. You must indicate whether you are creating an installation or deinstallation file, as the contents are different for each. You can use either of the following methods to create the file:
 - Create a response file containing all required parameter values and encrypted passwords. This file can be used right away. See ["Create a Response File With Values"](#) on page B-4 for instructions.
 - Create an empty response file. Before you can use this file, you must add all required encrypted passwords and clear-text parameter values, such as directory names and port numbers. See the following procedures for instructions:
 - ["Create an Empty Response File"](#) on page B-8
 - ["Add or Modify Clear-text Values in an Existing Response File"](#) on page B-10
 - ["Add or Modify Encrypted Passwords in an Existing Response File"](#) on page B-10
 3. Run the silent-mode installer or deinstaller. See the following procedures for instructions:
 - For installations, see ["Run the Silent-mode Installer"](#) on page B-13.
 - For deinstallations, see ["Run the Silent-mode Deinstaller"](#) on page B-15.
 4. To reuse the response file after a successful installation or deinstallation, you must reenter and encrypt passwords in the file. See ["Add or Modify Encrypted Passwords in an Existing Response File"](#) on page B-10 for instructions.

Silent Mode Tasks

Before using these tasks, see ["Silent Mode Process"](#) on page B-2 for an overview of the tasks and the order in which to use them.

- ["Start the Response File Build Utility"](#) on page B-4
- ["Create a Response File With Values"](#) on page B-4
- ["Create an Empty Response File"](#) on page B-8
- ["Add or Modify Clear-text Values in an Existing Response File"](#) on page B-10
- ["Add or Modify Encrypted Passwords in an Existing Response File"](#) on page B-10
- ["Run the Silent-mode Installer"](#) on page B-13
- ["Run the Silent-mode Deinstaller"](#) on page B-15

Start the Response File Build Utility

Use this procedure to prepare for using the response file build utility.

1. In a terminal window, connect to the STA server and log in as the Oracle install user. See ["Oracle install user"](#) on page 3-2 for details.
2. If you are creating a new response file, determine whether the directory where you plan to save it includes any response files you want to keep. 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 /ResponseFiles
$ ls -l *.rsp
-rw-r--r--  1 oracle  oracle                2836 Jun 30 16:49 silentInstall.rsp

$ mv silentInstall.rsp silentInstall_save.rsp
```

3. Change to the directory where the STA installer files have been downloaded; see ["Download STA"](#) on page 3-11 for details. For example:

```
$ cd /Installers
```

4. Launch the response file build utility. For example:

```
$ java -jar silentInstallUtility_2.2.0.3.30.jar
```

The utility starts and the Main Menu appears.

```
+-----+
| Main Menu           |
+-----+
```

Select Operation :

- 1) Create a new response file with prompts
- 2) Create an empty response file
- 3) Enter and encrypt passwords
- 4) Exit

Enter Choice [1-4] :

5. Make menu selections according to the tasks you want to perform. When you are finished using the utility, use the following steps to exit.
 - a. At the Press [Enter] to returning to Main Menu prompt, press Enter.
 - b. At the Main Menu, enter 4.

Create a Response File With Values

Use this procedure to create a response file containing all information needed for the STA silent-mode installer or deinstaller, including encrypted passwords. The response file build utility prompts you for the following information:

- Type of response file you want to create

- Directory where you want to save the file. The encryption key file will also be saved to this directory.
- All required parameters, including passwords. The requested parameters vary depending on the type of file you are creating. Passwords are not displayed on the screen, and they are encrypted before being added to the response file.

See ["Response File Utility Prompts and File Parameters"](#) on page B-17 for details about the requested information. The response file build utility does not verify your entries, and if they do not meet the parameter requirements, the silent installer or deinstaller may fail.

After performing this procedure, you can use the response file right away with the silent-mode installer or deinstaller. See ["Run the Silent-mode Installer"](#) on page B-13 or ["Run the Silent-mode Deinstaller"](#) on page B-15 for instructions.

1. Perform the necessary preparation steps and start the response file build utility. See ["Start the Response File Build Utility"](#) on page B-4 for details.
2. At the Main Menu, enter 1 to create a new response file with values.

```
+-----+
| Main Menu                |
+-----+
```

Select Operation :

- 1) Create a new response file with prompts
- 2) Create an empty response file
- 3) Enter and encrypt passwords
- 4) Exit

Enter Choice [1-4] : 1

The Create New Response File menu appears.

3. Enter the menu selection number for the type of response file you want to create.

```
+-----+
| Create New Response File |
+-----+
```

The utility will prompt the user for the values required to create a response file. The required passwords are then automatically encrypted and the file can be used immediately.

Select Response File type to create :

- 1) Silent Install
- 2) Silent De-install
- 3) Back to Main Menu

Enter Choice [1-3] :

The utility prompts for your input. The prompts vary based on the type of response file you have selected. See the following for details about your entries:

- [Table B-1, "Install Response File Reference"](#) on page B-17
 - [Table B-2, "Deinstall Response File Reference"](#) on page B-18
4. Respond to each prompt with the requested information. The password values you enter are not displayed on the screen. See the following examples for details:
 - [Example B-1, "Creating an Install Response File With Values"](#)

- [Example B-2, "Creating a Deinstall Response File With Values"](#)

Once you have entered all the required information, the utility creates the response file and displays its contents.

5. Exit the utility.

Example B-1 Creating an Install Response File With Values

Select Response File type to create :

- 1) Silent Install
- 2) Silent De-install
- 3) Back to Main Menu

Enter Choice [1-3] : **1**

The utility will now create a Silent Install response file.

The response file will be saved as <silentInstall.rsp>. If there is an existing file with the same name in the specified directory, the file will be overwritten.

Enter directory to save the response file to, or press <Enter> to save to the current directory :

The response file will be saved to : /Installers

```
+-----+
| Collecting User input |
+-----+
```

Enter location where STA will be installed (STORAGE_HOME). : **/Oracle**

Enter the System Root password :
 Confirm the System Root password :

Enter location for Database Data directory : **/dbdata**
 Enter location for Database Backup directory : **/dbbackup**

Enter Weblogic Administrator Username : **weblogic**
 Enter Weblogic Administrator Password :
 Confirm Weblogic Administrator Password :

Enter STA Administrator Username : **sta_admin**
 Enter STA Administrator Password :
 Confirm STA Administrator Password :

Enter STA Database Root User Password :
 Confirm Enter STA Database Root User Password :

Enter STA Database Application Username : **stadb**
 Enter STA Database Application Password :
 Confirm STA Database Application Password :

Enter STA Database Reports Username : **starrpt**
 Enter STA Database Reports Password :
 Confirm STA Database Reports Password :

Enter STA Database Administrator Username : **stadba**
 Enter STA Database Administrator Password :
 Confirm STA Database Administrator Password :

```

Enter WebLogic Administration Console HTTP Port      : 7019
Enter WebLogic Administration Console HTTPS Port     : 7020

Enter staEngine HTTP port                            : 7023
Enter staEngine HTTPS port                           : 7024

Enter staAdapter HTTP port                           : 7025
Enter staAdapter HTTPS port                          : 7026

Enter staUi HTTP port                                : 7021
Enter staUi HTTPS port                               : 7022

Enter RDA domain name                                : oracle.us.com
Creating keyfile /Installers/.sk1443544592068
[ENGINE]

# DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0

[GENERIC]
...
Complete contents of file
...
Response file generated. The file is located at /Installers/silentInstall.rsp

Press [Enter] to returning to Main Menu

```

Example B-2 Creating a Deinstall Response File With Values

```

Select Response File type to create :
  1) Silent Install
  2) Silent De-install
  3) Back to Main Menu

Enter Choice [1-3] : 2

The utility will now create a Silent Deinstall response file.

The response file will be saved as <silentDeinstall.rsp>. If there is an existing
file with the same name in the specified directory, the file will be overwritten.

Enter directory to save the response file to, or press <Enter> to save to the
current directory :

The response file will be saved to : /Installers

+-----+
| Collecting User input |
+-----+

Enter the System Root password      :
Confirm the System Root password    :
Creating keyfile /Installers/.sk1435706408183
...
Complete contents of file
...
Response file generated. The file is located at /Installers/silentDeinstall.rsp

Press [Enter] to returning to Main Menu

```

Create an Empty Response File

Use this procedure to create a response file containing placeholders for all information needed for the STA silent-mode installer or deinstaller. The response file build utility prompts you for the following information:

- Type of response file you want to create
- Directory where you want to save the file

After performing this procedure, you must use both of the following procedures, in either order, to supply all required values and make the response file usable:

- ["Add or Modify Clear-text Values in an Existing Response File"](#) on page B-10
 - ["Add or Modify Encrypted Passwords in an Existing Response File"](#) on page B-10
1. Perform the necessary preparation steps and start the response file build utility. See ["Start the Response File Build Utility"](#) on page B-4 for details.
 2. At the Main Menu, enter 2 to create a new empty response file.

```
+-----+
| Main Menu |
+-----+
```

Select Operation :

- 1) Create a new response file with prompts
- 2) Create an empty response file
- 3) Enter and encrypt passwords
- 4) Exit

Enter Choice [1-4] : **2**

The Generate Empty Response File menu appears.

3. Enter the selection number for the type of response file you want to create.

```
+-----+
| Generate Empty Response File |
+-----+
```

The utility will generate an empty response file with only the response file keys. The user is expected to fill in the values manually, then run the encrypt password function to encrypt the passwords before the response file can be used.

Select Response File type to generate :

- 1) Silent Install
- 2) Silent De-install
- 3) Back to Main Menu

Enter Choice [1-3] :

The utility prompts for the directory where you want to save the file.

4. At the directory prompt, specify an absolute path or press Enter. See the following examples for details:
 - [Example B-3, "Creating an Empty Install Response File"](#)
 - [Example B-4, "Creating an Empty Deinstall Response File"](#)

The utility creates the response file.

5. Exit the utility.

Example B-3 Creating an Empty Install Response File

```
+-----+
| Generate Empty Response File |
+-----+
```

The utility will generate an empty response file with only the response file keys. The user is expected to fill in the values manually, then run the encrypt password function to encrypt the passwords before the response file can be used.

Select Response File type to generate :

- 1) Silent Install
- 2) Silent De-install
- 3) Back to Main Menu

Enter Choice [1-3] : **1**

The utility will now generate an empty Silent Install response file.

The response file will be saved as <silentInstall.rsp>. If there is an existing file with the same name in the specified directory, the file will be overwritten.

Enter directory to save the response file to, or press <Enter> to save to the current directory :

The response file will be saved to : /Installers

Response file generated successfully.

The file is located at /Installers/silentInstall.rsp

Press [Enter] to returning to Main Menu

Example B-4 Creating an Empty Deinstall Response File

```
+-----+
| Generate Empty Response File |
+-----+
```

The utility will generate an empty response file with only the response file keys. The user is expected to fill in the values manually, then run the encrypt password function to encrypt the passwords before the response file can be used.

Select Response File type to generate :

- 1) Silent Install
- 2) Silent De-install
- 3) Back to Main Menu

Enter Choice [1-4] : **2**

The utility will now generate an empty Silent Deinstall response file.

The response file will be saved as <silentDeinstall.rsp>. If there is an existing file with the same name in the specified directory, the file will be overwritten.

Enter directory to save the response file to, or press <Enter> to save to the current directory :

The response file will be saved to : /Installers

Response file generated successfully.
The file is located at /Installers/silentDeinstall.rsp

Press [Enter] to returning to Main Menu

Add or Modify Clear-text Values in an Existing Response File

Use this procedure to manually add or change clear-text parameter values in an existing response file. You can perform this procedure on an empty file with just placeholders or one with values.

See "[Response File Utility Prompts and File Parameters](#)" on page B-17 for details about the required information.

Note: To ensure password security, do not enter clear-text passwords into the response file. Passwords must be encrypted. To add or modify passwords, see "[Add or Modify Encrypted Passwords in an Existing Response File](#)" on page B-10.

1. In a terminal window, connect to the STA server and log in as the Oracle install user. See "[Oracle install user](#)" on page 3-2 for details.
2. Use a text editor to edit the response file and provide values for the required clear-text parameters. Parameters vary depending on the type of response file. See "[Response File Utility Prompts and File Parameters](#)" on page B-17 for a detailed listing. Your entries must meet the parameter requirements, or the silent installer or deinstaller may fail.

Note: Do not manually modify passwords or other parameters that must be updated with the response file build utility.

3. Save and exit the file.

Add or Modify Encrypted Passwords in an Existing Response File

Use this procedure to add encrypted passwords to an existing response file. You can perform this procedure on a file with existing values or on an empty file with only placeholders. The file can be located in any directory and have any file name.

If you want to reuse a response file after a successful installation or deinstallation, you must use this procedure to reenter encrypted passwords.

The response file build utility prompts you for the following information:

- Type of response file you want to update
- Full path and file name of the response file you want to update. The encryption key file will be created in the same directory as the response file.
- All passwords for the response file type you have specified. Passwords are not displayed on the screen, and they are encrypted before being added to the response file.

See "[Response File Utility Prompts and File Parameters](#)" on page B-17 for details about the requested information. The response file build utility does not verify your entries, and if they do not meet the parameter requirements, the silent installer or deinstaller may fail.

1. Prepare for and start the response file build utility. See ["Start the Response File Build Utility"](#) on page B-4 for instructions.
2. At the Main Menu, enter 3 to add encrypted passwords to an existing response file.

```
+-----+
| Main Menu |
+-----+
```

Select Operation :

- 1) Create a new response file with prompts
- 2) Create an empty response file
- 3) Enter and encrypt passwords
- 4) Exit

Enter Choice [1-4] : 3

The Enter and Encrypt Passwords menu appears.

3. Enter the menu selection number for the type of response file you want to update.

```
+-----+
| Enter and encrypt passwords |
+-----+
```

The utility will prompt the user for the passwords required for the response file only, then generate the keyfile and encrypt the passwords. Existing values that are not passwords are ignored.

Select Response File type to encrypt :

- 1) Silent Install
- 2) Silent De-install
- 3) Back to Main Menu

Enter Choice [1-3] :

The utility prompts for the location of the file you want to update.

4. 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.

5. Respond to each prompt with the requested information. The password values you enter are not displayed on the screen. See ["Response File Utility Prompts and File Parameters"](#) on page B-17 for a detailed listing.

See the following examples for details:

- [Example B-5, "Adding Encrypted Passwords to an Install Response File"](#)
- [Example B-6, "Adding Encrypted Passwords to a Deinstall Response File"](#)

The utility adds the encrypted passwords to the response file and displays the file contents.

6. Exit the utility.

Example B-5 Adding Encrypted Passwords to an Install Response File

```
+-----+
| Enter and encrypt passwords |
```

```
+-----+
The utility will prompt the user for the passwords required for the response file
only, then generate the keyfile and encrypt the passwords. Existing values that
are not passwords are ignored.
```

```
Select Response File type to encrypt :
  1) Silent Install
  2) Silent De-install
  3) Back to Main Menu
```

```
Enter Choice [1-3] : 1
```

The utility will now encrypt your Silent Install response file passwords.

```
Enter the absolute location to the valid response file, including the filename :
/Installers/saved_silentInstall.rsp
```

```
Enter the System Root password           :
Confirm the System Root password         :
Enter Weblogic Administrator Password    :
Confirm Weblogic Administrator Password  :
Enter STA Administrator Password         :
Confirm STA Administrator Password       :
```

```
Enter STA Database Root User Password   :
Confirm Enter STA Database Root User Password :
Enter STA Database Application Password  :
Confirm STA Database Application Password :
Enter STA Database Reports Password     :
Confirm STA Database Reports Password   :
Enter STA Database Administrator Password :
Confirm STA Database Administrator Password :
```

```
Creating keyfile /Installers/.sk1436471175903
[ENGINE]
```

```
# DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0
...
Complete contents of file
...
Press [Enter] to returning to Main Menu
```

Example B-6 Adding Encrypted Passwords to a Deinstall Response File

```
+-----+
| Enter and encrypt passwords |
+-----+
The utility will prompt the user for the passwords required for the response file
only, then generate the keyfile and encrypt the passwords. Existing values that
are not passwords are ignored.
```

```
Select Response File type to encrypt :
  1) Silent Install
  2) Silent De-install
  3) Back to Main Menu
```

```
Enter Choice [1-4] : 2
```

The utility will now encrypt your Silent Deinstall response file passwords.

```
Enter the absolute location to the valid response file, including the filename :
/Installers/saved_silentDeinstall.rsp
```

```
Enter the System Root password           :
Confirm the System Root password        :
```

```
Creating keyfile /Installers/.sk1436471385123
[ENGINE]
```

```
# DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0
...
Complete contents of file
...
Press [Enter] to returning to Main Menu
```

Run the Silent-mode Installer

Use this procedure to install STA in silent mode.

1. In a terminal window, connect to the STA server and log in as the Oracle install user. See "[Oracle install user](#)" on page 3-2 for details.
2. Change to the STA installer location. For example:

```
$ cd /Installers
```

3. Start the STA silent-mode installer. See "[STA Installer and Deinstaller Command Options](#)" on page B-20 for full definitions of these parameters.

```
$ ./sta_installer_linux64_version.bin -silent -responseFile response_file
-invPtrLoc pointer_file
```

Where:

- *version* is the version of the STA installer you have downloaded.
- `-silent` indicates silent mode; this parameter is required.
- `-responseFile response_file` specifies the absolute path of the silent-mode installer response file; this parameter is required.
- `-invPtrLoc pointer_file` specifies the absolute path of the Oracle central inventory pointer file. This parameter is required only if there is no `/etc/orainst.loc` file or you want to use a different file.

For example:

```
$ ./sta_install_2.1.0.64.124_linux64.bin -silent -responseFile
/Installers/silentInstall.rsp -invPtrLoc /opt/oracle/orainst.loc
```

4. 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.

[Example B-7](#) shows the starting and ending messages that appear for a successful installation. [Example B-8](#) shows some messages you might see at the end of a failed installation.

5. When the installer completes successfully, verify that STA is running. See "[Verify Successful Installation](#)" on page 3-17 for instructions.

Example B-7 Successful STA Silent-mode Installation Sample Messages

```
./sta_install_2.2.0.3.30_linux64.bin -silent -responseFile /Installers/silentInstall.rsp
0%.....100%
Launcher log file is /tmp/OraInstall2015-07-17_10-45-24AM/launcher2015-07-17_10-45-24AM.log.
Starting Oracle Universal Installer

Checking if CPU speed is above 300 MHz.   Actual 2492.089 MHz   Passed
Checking swap space: must be greater than 512 MB.   Actual 8232956 MB   Passed
Checking temp space: must be greater than 4096 MB.   Actual 9124 MB   Passed
Checking for glibc version 2.12 .   Actual 2.12-1.107.el6.x86_64   Passed

Preparing to launch the Oracle Universal Installer from /tmp/OraInstall2015-07-17_10-45-24AM
Log: /tmp/OraInstall2015-07-17_10-45-24AM/install2015-07-17_10-45-24AM.log
Copyright (c) 2012, 2015, Oracle and/or its affiliates. All rights reserved.
Reading response file..
Starting check : CheckSTANotInstalled
Expected result: STA is not installed.
Actual Result: STA is not installed.
Check complete. The overall result of this check is: Passed
CheckSTANotInstalled Check: Success.
Starting check : CheckMysqlNotInstalled
Expected result: Package MySQL is not installed.
Actual Result: Package MySQL is not installed.
Check complete. The overall result of this check is: Passed
CheckMysqlNotInstalled Check: Success.

...

Started Configuration:Deploying STA Application
Configuration:Deploying STA Application completed successfully
Started Configuration:Restarting STA (this can take up to 30 minutes)
Configuration:Restarting STA (this can take up to 30 minutes) completed successfully
Started Configuration:Post Configuration
Log file successfully moved.
Configuration:Post Configuration completed successfully.
The installation of STA_Install 2.2.0.0.0 completed successfully.
Logs successfully copied to /home/oracle/oraInventory/logs.
$
```

Example B-8 Sample Failed STA Silent-mode Installation Final Messages

```
[ERROR] Rule_CalculateFreeSpace_Error. Aborting Install
Logs are located here: /tmp/OraInstall2014-09-24_09-29-29AM.
** Error during execution, error code = 256.
$
```

Run the Silent-mode Deinstaller

Use this procedure to deinstall the current version of STA using the silent-mode deinstaller. To deinstall an earlier version of STA, see that version of the *STA Installation and Configuration Guide*.

1. In a terminal window, connect to the STA server and log in as the Oracle install user. See ["Oracle install user"](#) on page 3-2 for details.
2. Change to the STA home directory. For example:


```
$ cd /Oracle/StorageTek_Tape_Analytics
```
3. Change to the STA utilities directory.


```
$ cd oui/bin
```
4. Start the STA silent-mode deinstaller. See ["STA Installer and Deinstaller Command Options"](#) on page B-20 for full definitions of these parameters.

```
$ ./deinstall.sh -silent -responseFile response_file -invPtrLoc pointer_file
```

Where:

- `-silent` indicates silent mode; this parameter is required.
- `-responseFile response_file` specifies the absolute path of the STA deinstaller response file; this parameter is required.
- `-invPtrLoc pointer_file` specifies the absolute path of the Oracle central inventory pointer file; this parameter is required only if the file does not exist in the `/etc` directory or you want to use a different file.

For example:

```
$ ./deinstall.sh -silent -responseFile /Installers/SilentDeinst.rsp
-invPtrLoc /opt/oracle/oraInst.loc
```

5. The deinstaller displays status messages in the terminal window as it deinstalls the STA application and data, MySQL, and WebLogic. See ["STA Deinstallation Overview"](#) on page 9-1 for details about the updates made. This process may take up to 30 minutes to complete.

[Example B-9](#) shows messages that appear for a successful deinstallation. [Example B-10](#) shows some messages you might see at the end of a failed deinstallation.

Example B-9 Sample Successful STA Silent-mode Deinstallation Messages

```
$ ./deinstall.sh -silent -responseFile /Installers/mysilentDeinstall.rsp
Launcher log file is /tmp/OraInstall2015-07-27_11-50-29AM/launcher2015-07-27_11-50-29AM.log.
Starting Oracle Universal Installer
```

```
Checking if CPU speed is above 300 MHz. Actual 2492.089 MHz Passed
Checking swap space: must be greater than 512 MB. Actual 8232956 MB Passed
Checking temp space: must be greater than 4096 MB. Actual 8528 MB Passed
Checking for glibc version 2.12 . Actual 2.12-1.107.el6.x86_64 Passed
```

```
Log: /tmp/OraInstall2015-07-27_11-50-29AM/deinstall2015-07-27_11-50-29AM.log
Setting ORACLE_HOME to /Oracle/StorageTek_Tape_Analytics
Copyright (c) 2012, 2015, Oracle and/or its affiliates. All rights reserved.
Reading response file..
Starting silent deinstallation...
```

```
-----20%-----40%-----60%-----80%-----
Successfully moved logs to /var/log/tbi/install.
s/common/bin/uninstall.sh/mysql was removed, with s/common/bin/uninstall.sh left, because there are
user defined files in s/common/bin/uninstall.sh or it is a mount point.
/dbdata/local was removed, with /dbdata left, because there are user defined files in /dbdata or it
is a mount point.
100%
```

The uninstall of STA_Install 2.2.0.0.0 completed successfully.
Logs successfully copied to /home/oracle/oraInventory/logs.

Example B-10 Sample Failed STA Silent-mode Deinstallation Final Messages

```
...
Reading response file..
Starting silent deinstallation...
-----20%-----40%-----60%-----80%-----
Internal Error: File Copy failed. Aborting Install
Logs are located here: /tmp/OraInstall2014-09-25_10-07-18AM.
```

6. When the deinstaller completes, verify that the STA directories have been removed. See ["Verify Successful Deinstallation"](#) on page 9-2 for instructions.

Response File Reference Information

See the following sections for details.

- ["Response File Build Utility Options"](#) on page B-16
- ["Sample Response Files"](#) on page B-18
- ["Response File Utility Prompts and File Parameters"](#) on page B-17

Response File Build Utility Options

The response file build utility provides the following options. See ["Start the Response File Build Utility"](#) on page B-4 for instructions on using the utility.

See ["Response File Utility Prompts and File Parameters"](#) on page B-17 for details about the requested information. The response file build utility does not verify your entries, and if they do not meet the parameter requirements, the silent installer or deinstaller may fail.

Create a new response file with prompts

This option creates a new response file with all required parameter values, including encrypted passwords. The utility prompts you for the values, and the created file is immediately usable. See ["Create a Response File With Values"](#) on page B-4 for instructions.

Create an empty response file

This option creates a response file with empty placeholders for all required parameters. Before using the file, you must provide the required clear-text values and encrypted passwords. See ["Create an Empty Response File"](#) on page B-8 for instructions.

Enter and encrypt passwords

This option adds encrypted passwords to an existing response file, which is either empty or has existing password values. The utility prompts you for the required passwords and adds them to the response file in encrypted form.

Use this option if you have a response file you have successfully used once and want to reuse. For security reasons, once a response file has been used for a successful installation or deinstallation, the encryption key file used to decrypt the passwords is deleted. Before reusing the response file, you must use this option to reenter and encrypt the passwords.

See ["Add or Modify Encrypted Passwords in an Existing Response File"](#) on page B-10 for instructions.

Response File Utility Prompts and File Parameters

The following tables provide reference information for updating response file parameter values.

- [Table B-1, "Install Response File Reference"](#) on page B-17
- [Table B-2, "Deinstall Response File Reference"](#) on page B-18

Table B-1 *Install Response File Reference*

Response File Build Utility Prompt	Parameter	Description
None	KEYFILE_LOC	Location of password encryption key file. Do not modify; automatically generated by response file build utility.
None	ORACLE_HOME	See "STA Home" on page A-9. Do not modify; automatically generated by response file build utility.
Enter location where STA will be installed (STORAGE_HOME)	STORAGE_HOME	See "Oracle Storage Home" on page A-8.
Enter the System Root password	ROOT_ACCESS_PASSWORD	See "Enter Root Password" on page A-14.
Enter location for Database Data directory	DBDATA_LOC	See "Database Data Location" on page A-15.
Enter location for Database Backup directory	DBBACKUP_LOC	See "Database Backup Location" on page A-15.
Enter Weblogic Administrator Username	WEBLOGIC_ADMIN_NAME	See "WebLogic Administrator" on page A-17.
Enter Weblogic Administrator Password	WEBLOGIC_ADMIN_PASSWORD	See "WebLogic Administrator" on page A-17. Modify with response file build utility only.
Enter STA Administrator Username	STAGUI_ADMIN_NAME	See "STA Administrator" on page A-18.
Enter STA Administrator Password	STAGUI_ADMIN_PASSWORD	See "STA Administrator" on page A-18. Modify with response file build utility only.
Enter STA Database Root User Password	MYSQL_ROOT_PASSWORD	See "Database Root User" on page A-20. Modify with response file build utility only.
Enter STA Database Application Username	MYSQL_APP_NAME	See "Database Application User" on page A-21.
Enter STA Database Application Password	MYSQL_APP_PASSWORD	See "Database Application User" on page A-21. Modify with response file build utility only.
Enter STA Database Reports Username	MYSQL_RPTS_NAME	See "Database Reports User" on page A-22.
Enter STA Database Reports Password	MYSQL_RPTS_PASSWORD	See "Database Reports User" on page A-22. Modify with response file build utility only.
Enter STA Database Administrator Username	MYSQL_DBA_NAME	See "Database Administrator" on page A-23.

Table B-1 (Cont.) Install Response File Reference

Response File Build Utility Prompt	Parameter	Description
Enter STA Database Administrator Password	MYSQL_DBA_PASSWORD	See "Database Administrator" on page A-23. Modify with response file build utility only.
Enter WebLogic Administration Console HTTP Port	ADMINSERVER_HTTP_PORT	See "WebLogic Admin Console" on page A-25.
Enter WebLogic Administration Console HTTPS Port	ADMIFNSERVER_HTTPS_PORT	
Enter staEngine HTTP port	STAENGINE_HTTP_PORT	See "STA Engine" on page A-26.
Enter staEngine HTTPS port	STAENGINE_HTTPS_PORT	
Enter staAdapter HTTP port	STAADAPTER_HTTP_PORT	See "STA Adapter" on page A-27.
Enter staAdapter HTTPS port	STAADAPTER_HTTPS_PORT	
Enter staUi HTTP port	STAU_HTTP_PORT	See "STA UI" on page A-28.
Enter staUi HTTPS port	STAU_HTTPS_PORT	
Enter RDA domain name	DOMAIN_NAME	See "Enter Domain Name" on page A-29.

Table B-2 Deinstall Response File Reference

Response File Build Utility Prompt	Parameter	Description
None	KEYFILE_LOC	Location of password encryption key file. Do not modify; automatically generated by response file build utility.
None	SELECTED_DISTRIBUTION	Do not modify; automatically generated by response file build utility.
Enter the System Root password	DEINSTALL_ROOT_ACCESS_PASSWORD	See "Enter Root Password" on page A-14. Modify with response file build utility only.

Sample Response Files

Following are sample response files with values.

- [Example B-11, "Sample Install Response File With Values"](#)
- [Example B-12, "Sample Deinstall Response File With Values"](#)

Example B-11 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=
# The Storage Home location. This can be an existing or new Storage Home.
STORAGE_HOME=
# 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+zaD3ZY44wwX3cwfzbzTw==
# Confirm Weblogic Administrator password. This needs to be encrypted using the
SilentInstallUtility
WEBLOGIC ADMIN CONFIRMPASSWORD=Ys+zaD3ZY44wwX3cwfzbzTw==
# 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=
# RDA Domain Name
DOMAIN NAME=
```

Example B-12 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/.sk1443552526409
# This will be blank when there is nothing to be de-installed in distribution
level
SELECTED_DISTRIBUTION=STA_Install~2.2.0.0.0
# System Root Password. This needs to be encrypted using the SilentInstallUtility
DEINSTALL ROOT ACCESS PASSWORD=68/gmu1W3EpFEE1XEln4zw==
# Confirm System Root Password. This needs to be encrypted using the
SilentInstallUtility
DEINSTALL ROOT ACCESS CONFIRM PASSWORD=68/gmu1W3EpFEE1XEln4zw==
```

STA Installer and Deinstaller Command Options

The following sections provide command reference information for the STA installer and deinstaller.

- ["Silent-mode Options"](#) on page B-20—Used exclusively with silent mode
- ["Logging Options"](#) on page B-21—Used with either graphical or silent mode
- ["Other Options"](#) on page B-21—Used with either graphical or silent mode

Silent-mode Options

The following options are used only with the silent-mode installer and deinstaller.

–force

Allow silent-mode installation into a non-empty directory.

–invPtrLoc *pointer_file*

Use 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 install group.

–response, –responseFile *response_file*

Required for silent mode. Location of the response file containing input for the STA silent-mode installer or deinstaller. *response_file* must be an absolute path.

–silent

Required for silent mode. Indicates to use silent mode. Inputs are taken from the specified response file.

Logging Options

The following options can be used with both the graphical and silent-mode installer and deinstaller. They allow you to control the types of information provided in the logs.

–debug

Log debug information. Some debug information will also appear in the console window.

–logLevel *level*

Omit log messages whose priority levels are lower than the specified level. Values for *level* are as follows:

- severe
- warning
- info
- config
- fine
- finer
- finest

–printdiskusage

Log debug information about disk usage.

–printmemory

Log debug information about memory usage.

–printtime

Log debug information about elapsed time.

Other Options

The following command options are for general use. They can be used with both graphical and silent modes.

–compatibilityFile *compatibility_file*

Location of the file that specifies feature set dependency changes.

–executeSysPrereqs

Execute the system environment prerequisite checks for running the installer, then exit without performing the installation.

–help

Display help.

–i, –install

Use graphical mode. This is the default.

-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.

-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.

Installation and Upgrade Worksheets

The worksheets in this appendix are planning tools to help you organize the activities and information you must gather to perform an STA installation or upgrade. This appendix includes the following sections:

- [Upgrade Preparation Worksheet](#)
- [Installation and Upgrade Worksheets](#)
- [Post-installation Configuration Worksheet](#)

Upgrade Preparation Worksheet

[Table C-1](#) is used only for upgrades from a previous version of STA. Use it to track the required and optional activities you perform to prepare for the upgrade. Use the "Comments" column to record any special planning information. See "[Preparation Tasks for All Upgrades](#)" on page 8-7 for complete details about these activities.

Table C-1 Upgrade Preparation Activities

Activity	Comments	Done
Verify current STA version is a released version. Note: If you are upgrading from STA 1.0.x, you must also install a new version of Linux before installing the new version of STA.		
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 filesystem for the upgrade.		
Review environment changes in the new version of STA or impact to your upgrade plan.		
Ensure all required RPM packages are installed (upgrades from STA 2.0.x only).		
Verify the current version of STA has recent, successful communication with the monitored libraries.		

Table C-1 (Cont.) Upgrade Preparation Activities

Activity	Comments	Done
Verify STA is processing exchanges across all monitored libraries.		
Move installation and database logs you wish to retain to a safe place (optional).		
Perform service log snapshot on current STA installation (optional).		
Download service log bundles you wish to retain (optional).		
Rename custom templates with "STA-" prefix (optional).		
Record current custom template settings you wish to retain (optional).		
Record Executive Report policy settings you wish to retain (optional).		

Installation and Upgrade Worksheets

These worksheets include information required by the STA installer. See "[Accounts and Ports Configured During STA Installation](#)" on page 3-3 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.

Installation Users and Locations Worksheet

[Table C-2](#) includes user accounts and locations you need to run the STA installer.

Table C-2 Installation Users and Locations Worksheet

Item	Description	Current Value	New Value
Oracle install group	Linux group used for installing and upgrading Oracle products on the STA server. Introduced in STA 2.1.0.	–	
Oracle install user	Linux user for installing and upgrading Oracle products on the STA server. Introduced in STA 2.1.0.	–	
Oracle central inventory location	Directory for tracking information about Oracle products installed on the STA server. Introduced in STA 2.1.0.	–	
Oracle storage home location	Directory where STA and associated Oracle software are installed. Introduced in STA 2.1.0.	–	

Table C-2 (Cont.) Installation Users and Locations Worksheet

Item	Description	Current Value	New Value
STA installer location	Location where the STA installer is downloaded.		
STA database data location	Location of the STA database.		
STA database backup location	Location of the STA database backups on the STA server.		

User Accounts Worksheet

Table C-3 includes user accounts you will use to perform STA administration activities, and MySQL accounts used internally by the STA application to access and manage the STA database.

Note: Password requirements have changed for STA 2.2.x. See ["Username and Password Requirements"](#) on page 3-3 for details.

Table C-3 User Accounts Worksheet

Account	Description	Current Username and Password	New Username and Password
WebLogic Administration	Used to log in to the WebLogic Administration console. Caution: The username and password for this account are not retrievable. If these credentials are lost, STA must be re-installed.		
STA Administrator	Used to log in to the STA application with full access privileges.		
STA Database Root User	Owns the MySQL database. The predefined username of root cannot be changed. Caution: The password for this account is not retrievable.	username = root	username = root
STA Database Application User	STA uses this account to connect to the database.		
STA Database Reports User	Non-STA and third-party applications use this account to connect to the database.		
STA Database Administrator User	STA administration and monitoring utilities use this account to connect to the database, primarily to perform scheduled backups.		

Port Number Worksheets

Table C-4 includes external ports used by the STA application. These port numbers are predefined and cannot be changed. Use the "Verified" column to record that you have verified with your network administrator that these ports are open and available.

Table C-4 Unconfigurable External Ports

Port Description	Protocol	STA Port	Verified
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.	SNMPTRAP	162	

Table C-5 includes configurable external and internal ports used by the STA application. Use the "Verified" column to record that you have verified 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-5 Configurable Internal and External Ports

Port Description	Type	Protocol	Default Port for STA 2.1.0 & Later	Current Port	New Port	Verified
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			

Domain Name Worksheet

Table C-6 includes your site's fully qualified domain name used by Oracle's Remote Diagnostic Agent (RDA) when generating STA service logs.

Table C-6 Company Domain Name

Required Information	Current Value	New Value
Company domain name (for example, us.example.com)		

Post-installation Configuration Worksheet

Table C-7 includes information you use 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 ["Configuring the SNMP v3 Protocol on the Libraries"](#) on page 5-1 for complete details about the requested information.

Table C-7 SNMP v3 User Configuration Information

Required Information	Current Values	New Values
SNMP v3 Username		
SNMP v3 Authorization Password (Auth)		
SNMP v3 Privacy Encryption Password (Privacy)		
SNMP v2c User Community		
SNMP v2c Trap Community		

Configuring Security Certificates

Oracle supplies self-generated security certificates to be used with HTTPS/SSL ports. During installation, STA uses the Java keytool to generate a certificate on the STA server, using the server hostname. You can optionally replace the Oracle certificate with your own approved certificate from a selected certificate authority (for example, VeriSign).

This chapter includes the following section:

- [Security Certificate Configuration Tasks](#)

Security Certificate Configuration Tasks

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"](#) on page D-1
- ["Reconfigure WebLogic to use a Different Security Certificate"](#) on page D-2
- ["Replace the Oracle Certificate"](#) on page D-9

Note: These procedures use Mozilla Firefox running on a Windows platform.

Establish the Initial HTTPS/SSL Connection

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*:*port_number*/STA/

Where:

- *host_name* is the hostname of the STA server.
- *port_number* 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/`

The Connection is Untrusted screen appears.

2. Select **I Understand the Risks**, and then click **Add Exception**.

The Add Security Exception screen appears.

3. Click View.

The Certificate Viewer screen appears. The certificate is *not* shown as verified because it is not from a certificate authority.

4. To examine the certificate, click the Details tab.

5. In the Certificate Fields panel, select issuer. Following is a sample display. CN indicates the server name on which the certificate was generated.

```
CN = staserver.example.com
OU = Tape Systems
O = Oracle America Inc
L = Redwood City
ST = California
C = USA
```

6. Click Close to return to the Add Security Certificate screen.

7. Select Confirm Security Exception.

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

1. Start a supported Web browser on your computer.

2. In the Location Bar or Address field, 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`

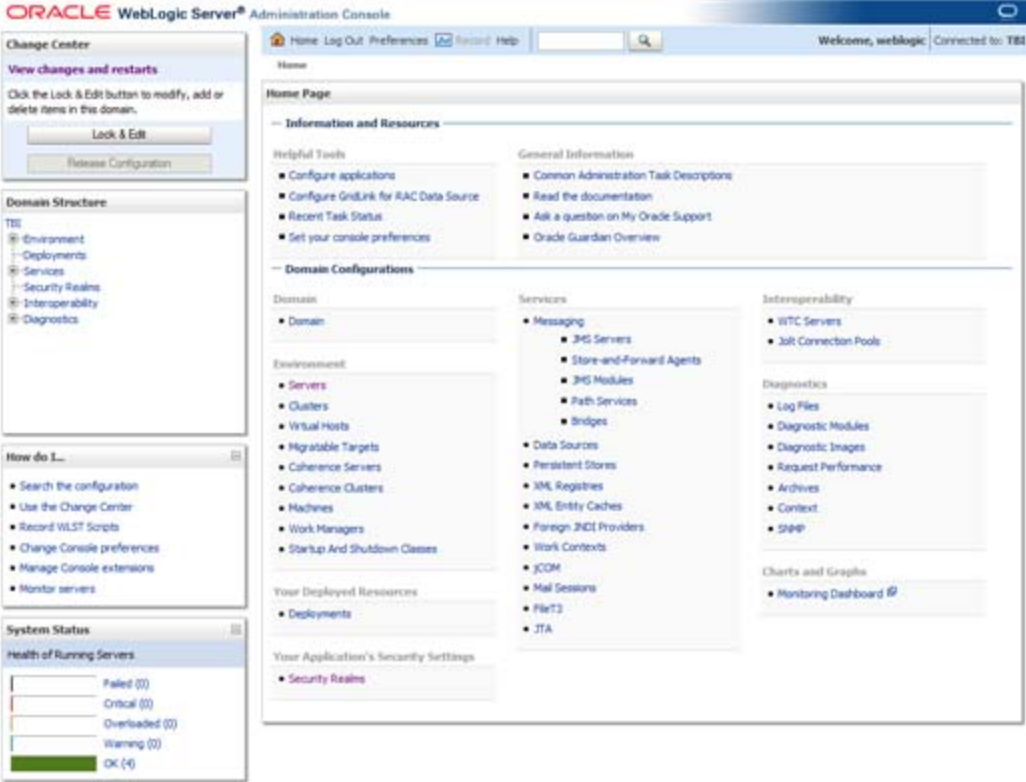
where *local_host_name* and *port_number* are the name and port number of the WebLogic Administrator console defined during STA installation. The default HTTP port number is 7019, and the default HTTPS port number is 7020. For example:

`https://sta_server:7020/console`

3. On the Welcome screen, enter the WebLogic Administration console username and password defined during STA installation, and then click Login.



The WebLogic Server Administration Console Home page appears.



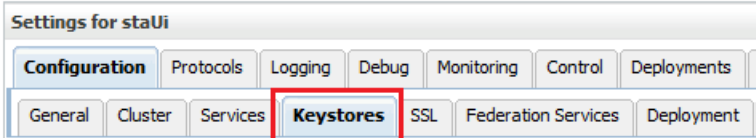
4. In the Domain Structure section, select **Environment**, and then select **Servers**.



5. In the Servers table, select the **staUi** active link (select the name itself, not the check box).

<input type="checkbox"/>	Name	Cluster	Machine
<input type="checkbox"/>	AdminServer(admin)		
<input type="checkbox"/>	staAdapter	STA_Cluster1	
<input type="checkbox"/>	staEngine	STA_Cluster1	
<input type="checkbox"/>	staUi	STA_Cluster1	

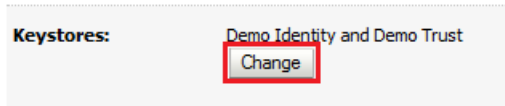
6. Select the **Keystores** tab.



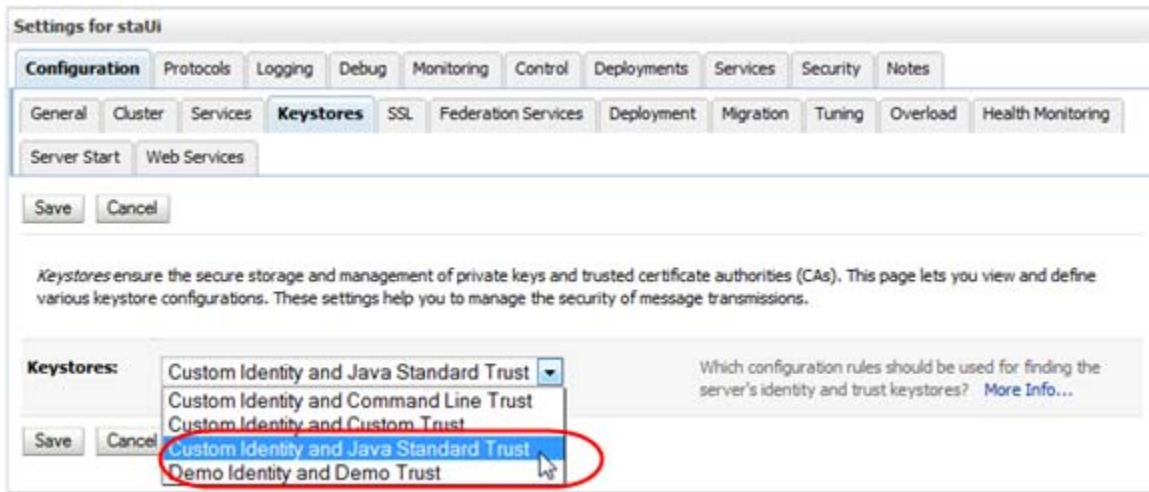
7. In the Change Center section, click **Lock & Edit**.



8. In the Keystores section, click **Change**.



9. In the **Keystores** menu, select Custom Identity and Java Standard Trust.



10. Click **Save**.

11. 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 re-install STA.

Settings for staUi

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services **Keystores** SSL Federation Services Deployment Migration Tuning Overload Health Monitoring

Server Start Web Services

Save

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

Keystores: Custom Identity and Java Standard Trust Which configuration rules should be used for finding the server's identity and trust keystores? [More Info...](#)
[Change](#)

— Identity —

Custom Identity Keystore: The path and file name of the identity keystore. [More Info...](#)

Custom Identity Keystore Type: The type of the keystore. Generally, this is JKS. [More Info...](#)

Custom Identity Keystore Passphrase: The encrypted custom identity keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. [More Info...](#)

Confirm Custom Identity Keystore Passphrase:

— Trust —

Java Standard Trust Keystore: The path and file name of the trust keystore. [More Info...](#)

Java Standard Trust Keystore Type: The type of the keystore. Generally, this is JKS. [More Info...](#)

Java Standard Trust Keystore Passphrase: The password for the Java Standard Trust keystore. This password is defined when the keystore is created. [More Info...](#)

Confirm Java Standard Trust Keystore Passphrase:

Save

12. Click **Save**.
13. Select the **SSL** tab.

Settings for staUi

Configuration Protocols Logging Debug Monitoring Control

General Cluster Services Keystores **SSL** Federation Services

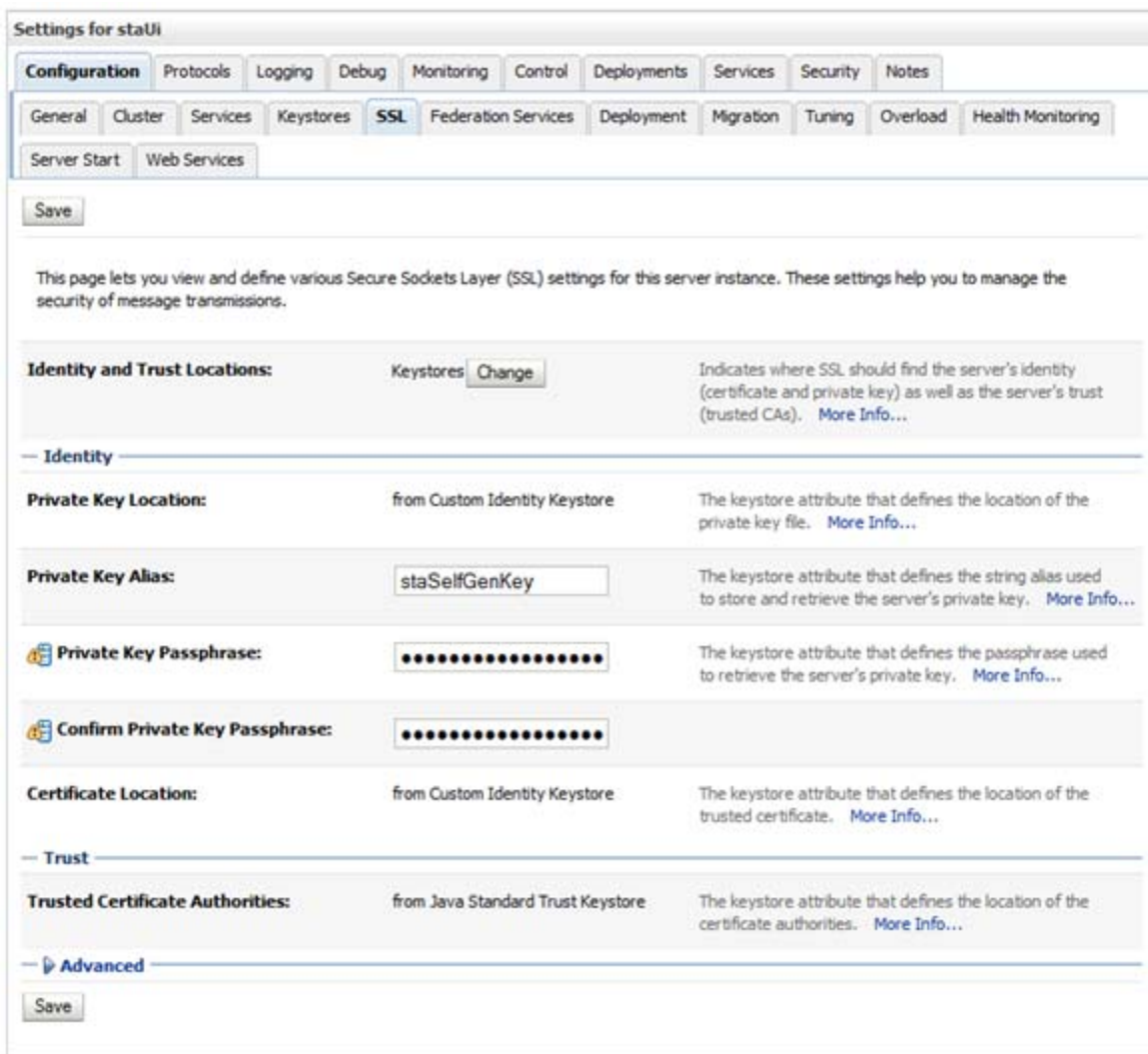
14. Enter the **Private Key Alias** and **Private Key Passphrase** supplied by the MVS system programmer.

Note: 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
```



15. Click **Save**.

16. In the Trusted Certificate Authorities section, click **Advanced**.

Settings for stali

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores **SSL** Federation Services Deployment Migration Tuning Overload Health Monitoring

Server Start Web Services

Save

This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instance. These settings help you to manage the security of message transmissions.

Identity and Trust Locations: Keystores [Change](#) Indicates where SSL should find the server's identity (certificate and private key) as well as the server's trust (trusted CA). [More Info...](#)

— Identity

Private Key Location: From Custom Identity Keystore The keystore attribute that defines the location of the private key file. [More Info...](#)

Private Key Alias: The keystore attribute that defines the string alias used to store and retrieve the server's private key. [More Info...](#)

Private Key Passphrase: The keystore attribute that defines the passphrase used to retrieve the server's private key. [More Info...](#)

Confirm Private Key Passphrase:

Certificate Location: From Custom Identity Keystore The keystore attribute that defines the location of the trusted certificate. [More Info...](#)

— Trust

Trusted Certificate Authorities: From Java Standard Trust Keystore The keystore attribute that defines the location of the certificate authorities. [More Info...](#)

[Advanced](#)

17. 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.

Advanced

Hostname Verification: BEA Hostname Verifier Specifies whether to ignore the installed implementation of the `weblogic.security.SSL.HostnameVerifier` interface (when this server is acting as a client to another application server). [More Info...](#)

Custom Hostname Verifier: The name of the class that implements the `weblogic.security.SSL.HostnameVerifier` interface. [More Info...](#)

Export Key Lifespan: 500 Indicates the number of times WebLogic Server can use an exportable key between a domestic server and an exportable client before generating a new key. The more secure you want WebLogic Server to be, the fewer times the key should be used before generating a new key. [More Info...](#)

Use Server Certs Sets whether the client should use the server certificates/key as the client identity when initiating an outbound connection over https. [More Info...](#)

Two Way Client Cert Behavior: Client Certs Requested But Not Enforced The form of SSL that should be used. [More Info...](#)

Cert Authenticator: The name of the Java class that implements the `weblogic.security.acl.CertAuthenticator` class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. [More Info...](#)

SSLRejection Logging Enabled Indicates whether warning messages are logged in the server log when SSL connections are rejected. [More Info...](#)

Allow Unencrypted Null Cipher Test if the `AllowUnEncryptedNullCipher` is enabled. [More Info...](#)

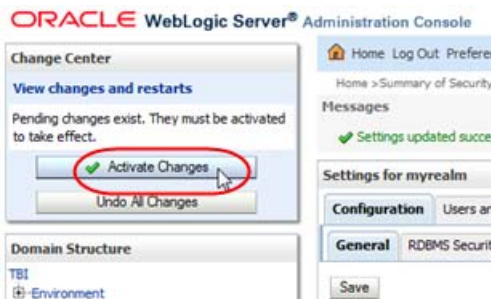
Inbound Certificate Validation: Builtin SSL Validation Only Indicates the client certificate validation rules for inbound SSL. [More Info...](#)

Outbound Certificate Validation: Builtin SSL Validation Only Indicates the server certificate validation rules for outbound SSL. [More Info...](#)

Use JSSE SSL Select the JSSE SSL implementation to be used in Weblogic. [More Info...](#)

18. Click **Save**.

19. In the Change Center section, click **Activate Changes**.



20. Log out of WebLogic.

21. Stop all STA services. See the *STA Administration Guide* for command usage details.

```
# STA stop all
Stopping the stau service.....
Successfully stopped the stau service
Stopping the staadapter service.....
Successfully stopped the staadapter service
Stopping the staengine service.....
Successfully stopped the staengine service
Stopping the stawebllogic service.....
Successfully stopped the stawebllogic service
Stopping the staservd Service...
Successfully stopped staservd service
Stopping the mysql service.....
Successfully stopped mysql service
#
```

22. Start all STA services.

```
# STA start all
Starting mysql Service..
mysql service was successfully started
Starting staservd Service.
staservd service was successfully started
Starting stawebllogic service.....
stawebllogic service was successfully started
Starting staengine Service.....
staengine service was successfully started
Starting staadapter Service.....
staadapter service was successfully started
Starting stau Service.....
stau service was successfully started
#
```

Replace the Oracle 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:port_number/STA/
```

Where:

- *host_name* is the hostname of the STA server.
- *port_number* 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. Select **I Understand the Risks** on the This Connection is Untrusted screen.
3. Click **Add Exception**.
4. To specify a certificate for your organization, click **Get Certificate** on the Add Security Certificate screen and select the appropriate file.
5. Click **Confirm Security Exception**.

Configuring External Authentication Providers for STA

This appendix describes how to configure Oracle's WebLogic Server to use one or more external authentication providers to authenticate users for STA. It includes the following sections:

- [Understanding the WebLogic Server Active Security Realm](#)
- [Considerations for Configuring External Authentication Providers](#)
- [Authentication Provider Configuration Process Overview](#)
- [Tasks for Configuring Active Directory and OpenLDAP Authentication Providers](#)
- [Tasks for Configuring IBM RACF Authentication Providers](#)

See *Fusion Middleware Securing Oracle WebLogic Server* for complete details about managing user authentication with WebLogic Server.

To create users from within the STA application, see the *STA User's Guide*.

Understanding the WebLogic Server Active Security Realm

WebLogic Server, which is included in the STA installation, manages all user authentication for STA. The STA installation includes one WebLogic Server active security realm, named `myrealm`. All authentication providers for STA must be defined in this 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.

Note: Do not change the names of the `myrealm` security realm and the `DefaultAuthenticator`; these names are required for STA.

Note: The active security realm also includes a provider named `DefaultIdentityAsserter`. Do not make any changes to this provider.

Considerations for Configuring External Authentication Providers

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.

The following sections provide information for configuring external authentication providers for STA.

- ["Supported Authentication Provider Types"](#) on page E-2
- ["Using the WebLogic Administration Console"](#) on page E-2
- ["LDAP Principal User"](#) on page E-2
- ["STA Access Group"](#) on page E-3
- ["Default STA User Role"](#) on page E-3
- ["Configuring the Authentication Process for Multiple Providers"](#) on page E-3
- ["LDAP Authentication Referrals"](#) on page E-3
- ["Using SSL for Communications"](#) on page E-4

Supported Authentication Provider Types

STA supports the following authentication provider types:

- OpenLDAP
- Microsoft Active Directory (AD)
- IBM Resource Access Control Facility (RACF)

Using the WebLogic Administration Console

Use the WebLogic Administration console for all STA authentication provider configuration tasks in WebLogic Server. See ["Edit the WebLogic Server Active Security Realm"](#) on page E-5 for instructions.

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 Server, this user is called the *Principal* user. You can either create a new user account for this purpose or use an existing one. See ["Prepare the External Authentication Provider for STA Authentication"](#) on page E-5 for instructions.

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 (see ["STA Access Group"](#) on page E-3, below).

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. See "[Prepare the External Authentication Provider for STA Authentication](#)" on page E-5 for instructions.

Default STA User Role

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 details about STA user roles.

Configuring the Authentication Process for Multiple Providers

When configuring multiple authentication providers, you can use the following options to control how WebLogic Server uses the providers in the authentication process.

Authentication Provider Order

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. See "[Task 4: Ensure Proper Order of Authentication Providers](#)" on page E-17 for instructions.

Note: The `DefaultAuthenticator` and the `DefaultIdentityAsserter` must be the first two providers in the list.

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`. See "[Task 3: Set the JAAS Control Flag](#)" on page E-15 for instructions.

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.

LDAP Authentication Referrals

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 you verify the setting. See ["Task 2: Define Provider-specific Information"](#) on page E-10 for instructions.

Using SSL for Communications

If the connection between WebLogic Server and the external authentication server is to be secured through SSL, you must perform the following activities:

- Ensure that the `SSLEnabled` attribute is selected on the Provider Specific screen. See ["Task 2: Define Provider-specific Information"](#) on page E-10 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.

Authentication Provider Configuration Process Overview

This section summarizes the tasks required to configure one or more external authentication providers for STA. See the referenced tasks for detailed instructions.

1. Prepare the external provider to authenticate STA users, and gather configuration information required by WebLogic Server. See ["Prepare the External Authentication Provider for STA Authentication"](#) on page E-5 for instructions.
2. Configure WebLogic Server to use external authentication providers. For each provider, perform all of the following tasks in the order indicated.
 - a. Add the external authentication provider to the WebLogic active security realm. See ["Task 1: Add an External Authentication Provider"](#) on page E-8 for instructions.
 - b. Configure provider-specific information for the authentication provider. See ["Task 2: Define Provider-specific Information"](#) on page E-10 for instructions.
 - c. Set the JAAS control flag for the provider. See ["Task 3: Set the JAAS Control Flag"](#) on page E-15 for instructions.
 - d. Ensure WebLogic Server will call all authentication providers in the order you want. See ["Task 4: Ensure Proper Order of Authentication Providers"](#) on page E-17 for instructions.
 - e. Apply the changes to WebLogic Server and STA. See ["Task 5: Apply All Configuration Changes"](#) on page E-19 for instructions.
3. Verify the configuration. See ["Verify Configuration of Authentication Providers"](#) on page E-21 for instructions.

Tasks for Configuring Active Directory and OpenLDAP Authentication Providers

Use the following procedures to configure OpenLDAP and Microsoft Active Directory authentication providers. To configure IBM RACF providers, see ["Tasks for Configuring IBM RACF Authentication Providers"](#) on page E-23.

- ["Prepare the External Authentication Provider for STA Authentication"](#) on page E-5
- ["Edit the WebLogic Server Active Security Realm"](#) on page E-5
- ["Task 1: Add an External Authentication Provider"](#) on page E-8

- ["Task 2: Define Provider-specific Information"](#) on page E-10
- ["Task 3: Set the JAAS Control Flag"](#) on page E-15
- ["Task 4: Ensure Proper Order of Authentication Providers"](#) on page E-17
- ["Task 5: Apply All Configuration Changes"](#) on page E-19
- ["Verify Configuration of Authentication Providers"](#) on page E-21

Prepare the External Authentication Provider for STA Authentication

Use this procedure to 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. See ["LDAP Principal User"](#) on page E-2 for details.
2. Create the STA access group. This group must have the name `StorageTapeAnalyticsUser`. See ["STA Access Group"](#) on page E-3 for details.
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 ["Task 2: Define Provider-specific Information"](#) on page E-10 for examples of the information to gather.

Edit the WebLogic Server Active Security Realm

This procedure provides general instructions for logging in to the WebLogic Administration console and making changes to the WebLogic Server active security realm.

1. Start a supported Web browser on your computer.
2. In the **Location Bar** or **Address** field, 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`

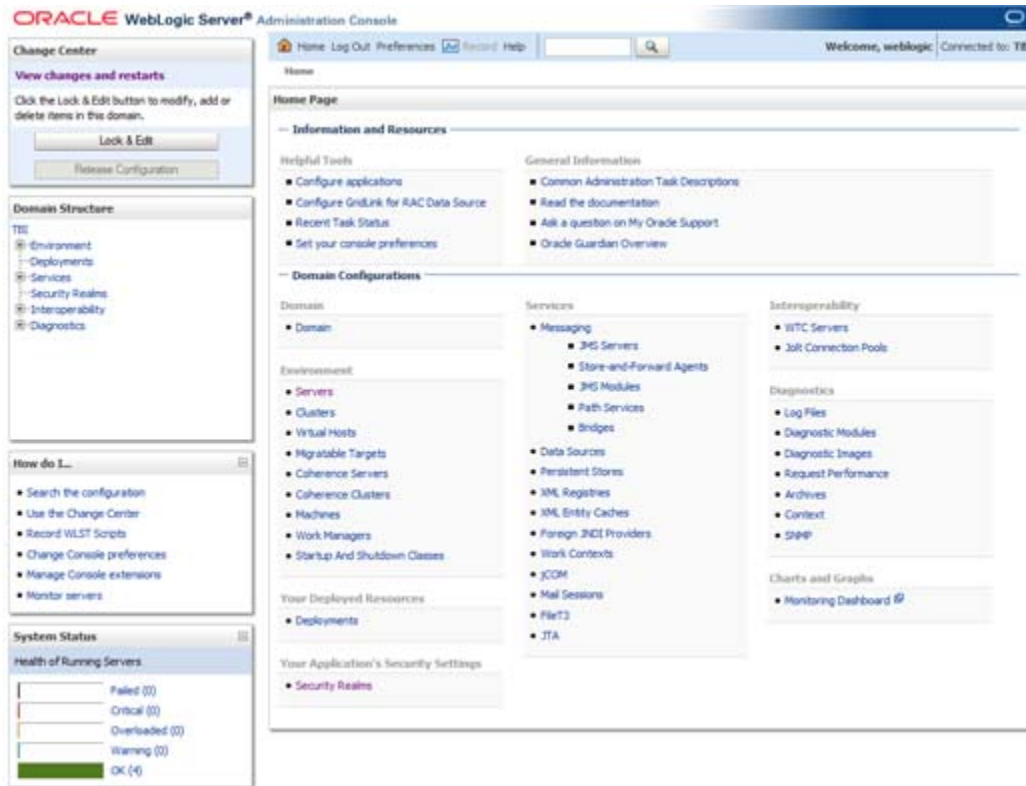
where *local_host_name* and *port_number* are the name and port number of the WebLogic Administrator console defined during STA installation. The default HTTP port number is 7019, and the default HTTPS port number is 7020. For example:

`https://sta_server:7020/console`

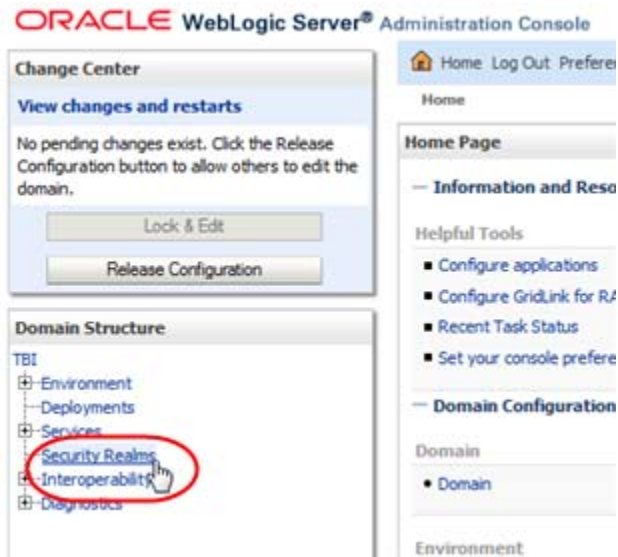
3. On the Welcome screen, enter the WebLogic Administration console username and password defined during STA installation, and then click **Login**.



The WebLogic Server Administration Console Home page appears.



4. Use the following steps to access the active security realm.
 - a. In the Domain Structure navigation tree, select **Security Realms**.

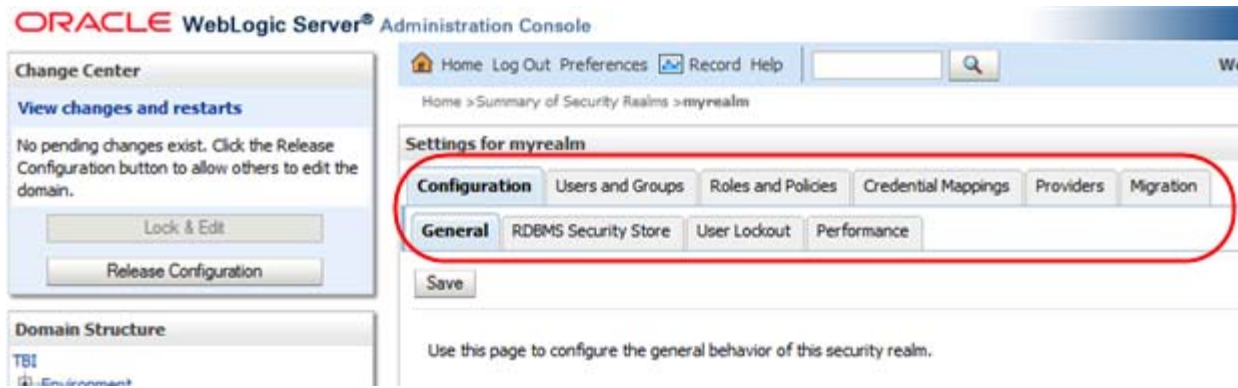


b. In the Realms table, select the **myrealm** active link.



The Settings for myrealm screen appears.

5. Use the tabs in the control bar to navigate to the screens you want to edit. You can make changes to multiple screens during a single editing session.



6. Use the Change Center section as follows:
 - To make changes to the screens, you must click **Lock & Edit**. This locks out other users from making changes at the same time.

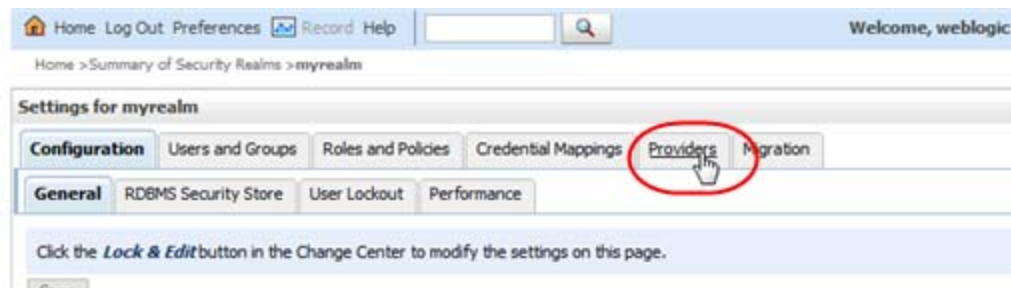


- When you have finished editing each screen, click **Save** to keep the changes or **Release Configuration** to cancel them.
 - When you have finished your editing session, click **Activate Changes** to apply all changes to all screens.
 - At any time during your editing session, you can click **Undo All Changes** to cancel all changes to all screens.
7. For your changes to take effect in STA, you must log out of the WebLogic Administration console and stop and restart STA. See "[Task 5: Apply All Configuration Changes](#)" on page E-19 for instructions.

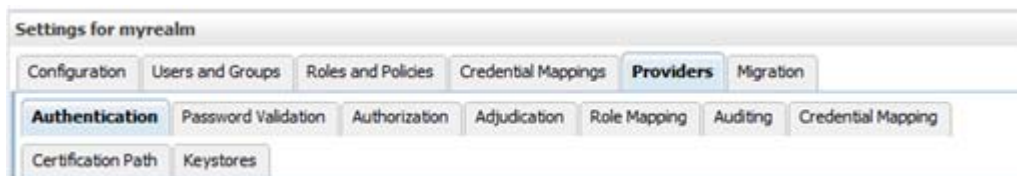
Task 1: Add an External Authentication Provider

Use this procedure to add an external authentication provider to the WebLogic Server active security realm.

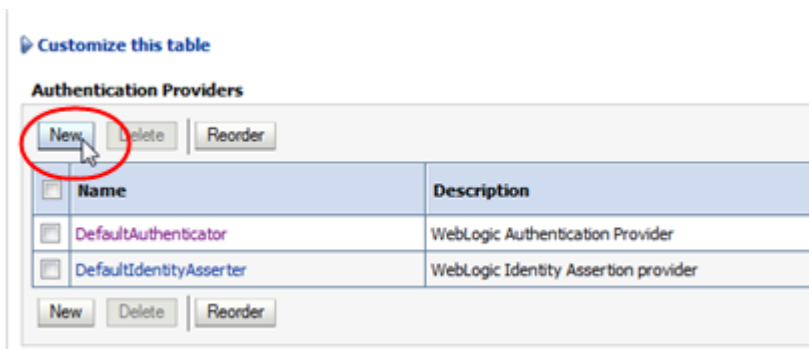
1. If you have not done so already, access the active security realm and lock it from other users. See "[Edit the WebLogic Server Active Security Realm](#)" on page E-5 for instructions
2. In the Settings for myrealm control bar, select the **Providers** tab.



The **Authentication** secondary tab is selected by default.



3. In the Authentication Providers table, click **New**.



4. Complete the Create a New Authentication Provider screen as follows, and then click **OK**.
 - **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.

Create a New Authentication Provider

OK Cancel

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.

* Indicates required fields

The name of the authentication provider.

* Name:

This is the type of authentication provider you wish to create.

Type:

OK Cancel

The external authentication provider is added to bottom of the Authentication Providers table.

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings **Providers** Migration

Authentication Password Validation Authorization Adjudication Role Mapping Auditing Credential Mapping

Certification Path Keystores

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows you to work with users and groups from previous releases of WebLogic Server.

Customize this table

Authentication Providers

New Delete Reorder Showing 1 to 3 of 3 Previous | Next

<input type="checkbox"/>	Name	Description	Version
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider	1.0
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
<input type="checkbox"/>	My AD Server	Provider that performs LDAP authentication	1.0

New Delete Reorder Showing 1 to 3 of 3 Previous | Next

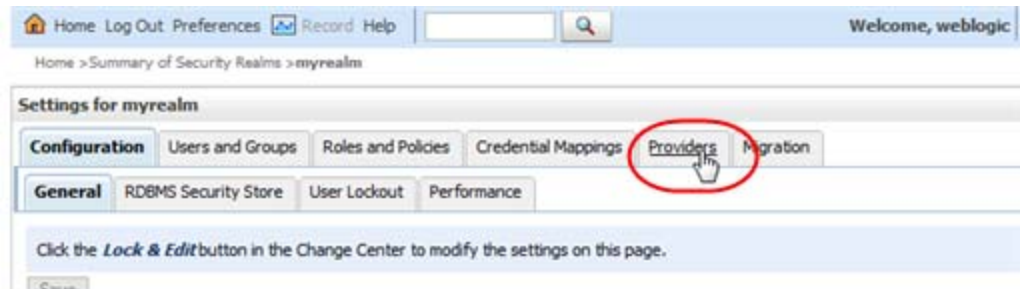
5. Proceed to "Task 2: Define Provider-specific Information" on page E-10.

Task 2: Define Provider-specific Information

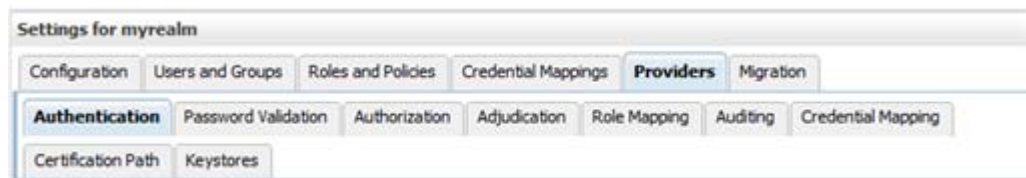
Use this procedure to define provider-specific information for each external authentication provider you have added to the WebLogic Server active security realm.

Before using this procedure, you must gather the necessary configuration information from the external authentication provider; see "Prepare the External Authentication Provider for STA Authentication" on page E-5 for instructions.

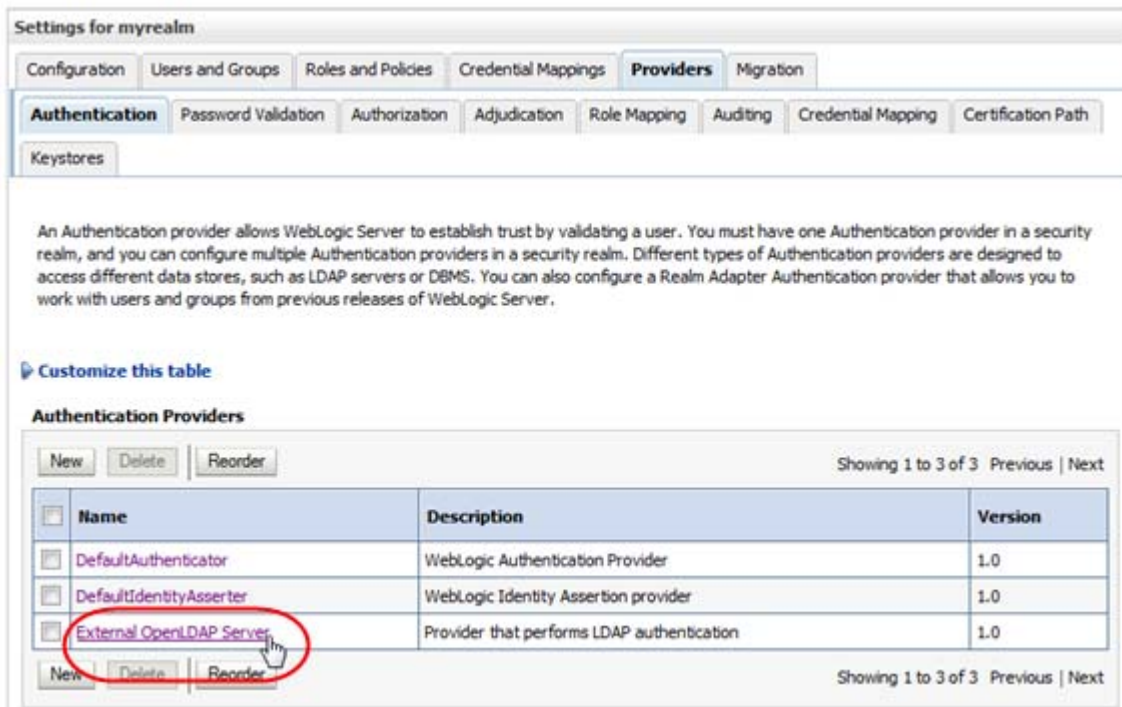
1. If you have not done so already, access the active security realm and lock it for editing. See ["Edit the WebLogic Server Active Security Realm"](#) on page E-5 for instructions.
2. In the Settings for myrealm control bar, select the **Providers** tab.



The **Authentication** secondary tab is selected by default.

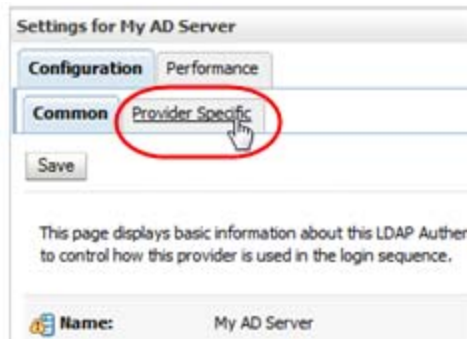


3. In the Authentication Providers table, select the active link for the provider you want to configure.

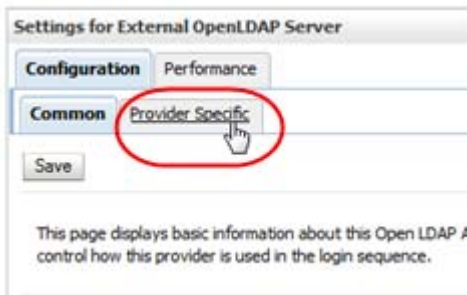


The Settings for authenticator screen appears.

4. In the control bar, select the **Configuration** tab and then the **Provider Specific** secondary tab.



The Provider Specific screen appears.



5. 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. See "[LDAP Principal User](#)" on page E-2 for details.
- **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 "[Using SSL for Communications](#)" on page E-4 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. See "[LDAP Authentication Referrals](#)" on page E-3 for details.

[Example E-1](#) and [Example E-2](#) 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 with entry syntax.

6. When you have finished entering screen values, click **Save**.



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 DN's 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 DN 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

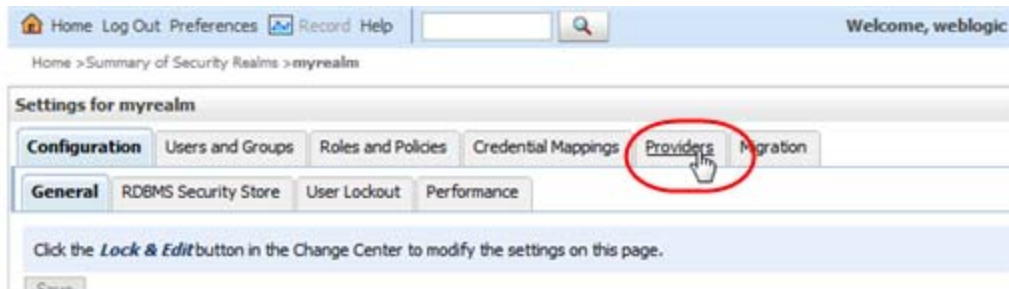
7. Proceed to ["Task 3: Set the JAAS Control Flag"](#) on page E-15.

Task 3: Set the JAAS Control Flag

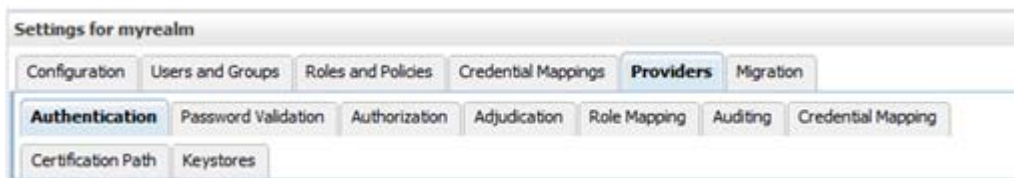
Use this procedure to set the JAAS control flag to indicate how WebLogic Server will use each provider in the user authentication process. See ["JAAS Control Flag"](#) on page E-3 for details.

Note: You must perform this procedure for all authentication providers, including the DefaultAuthenticator. Do *not* perform this procedure for the DefaultIdentityAsserter.

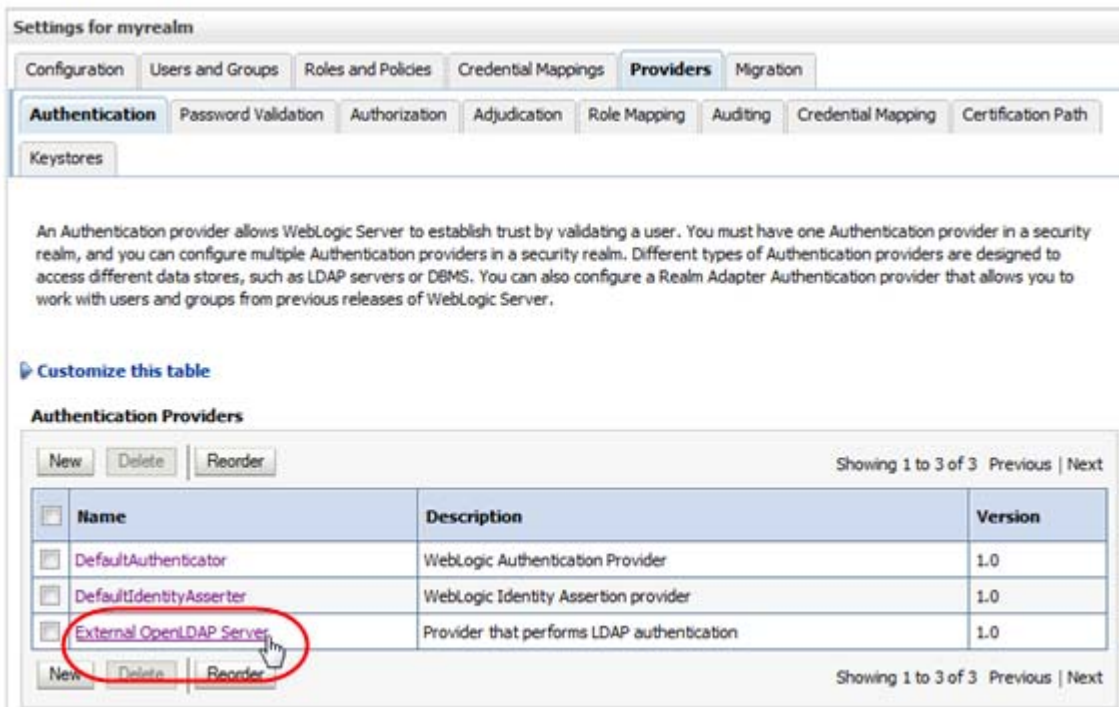
1. If you have not done so already, access the active security realm and lock it for editing. See "Edit the WebLogic Server Active Security Realm" on page E-5 for instructions.
2. In the Settings for myrealm control bar, select the **Providers** tab.



The **Authentication** secondary tab is selected by default.

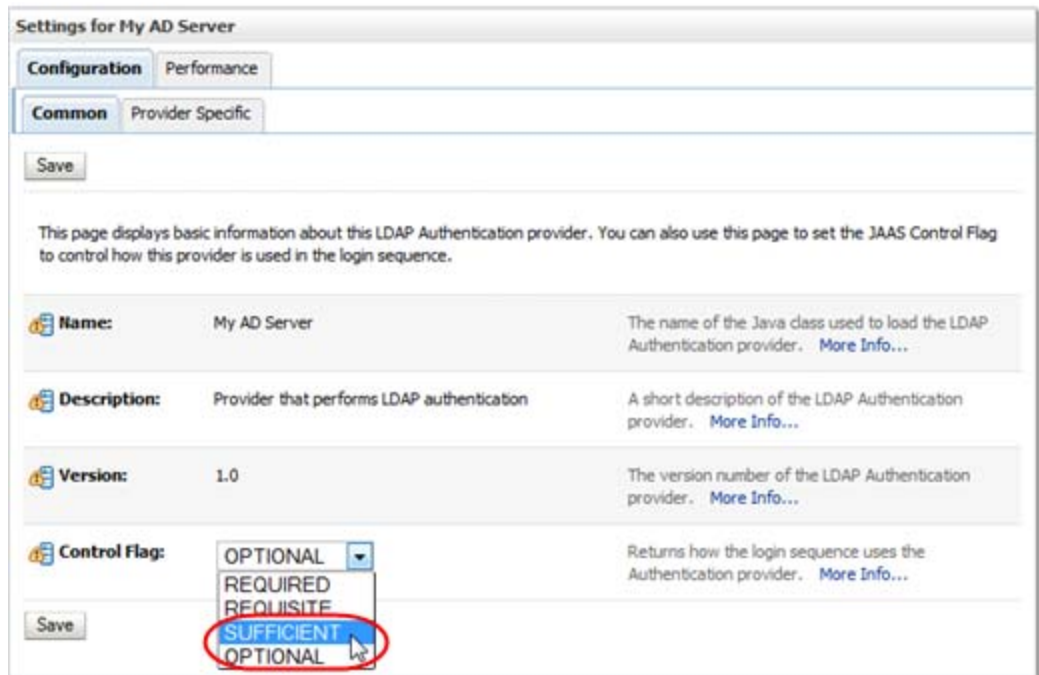


3. In the Authentication Providers table, select the active link for the provider you want to update.



The **Configuration** tab and **Common** secondary tab are selected by default.

4. In the **Control Flag** menu, select Sufficient.

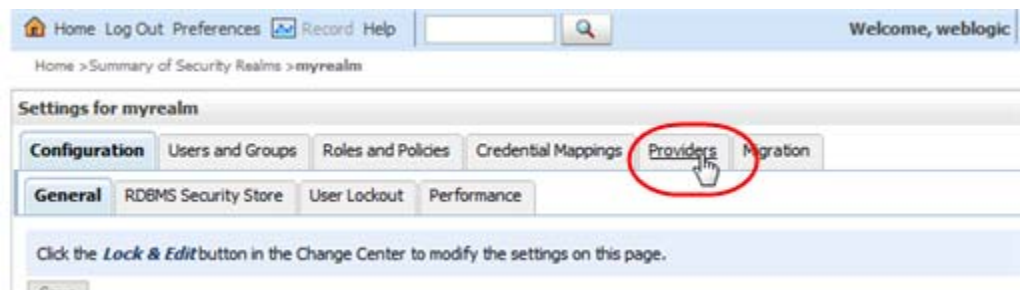


5. Click **Save**.
6. Proceed to "[Task 4: Ensure Proper Order of Authentication Providers](#)" on page E-17.

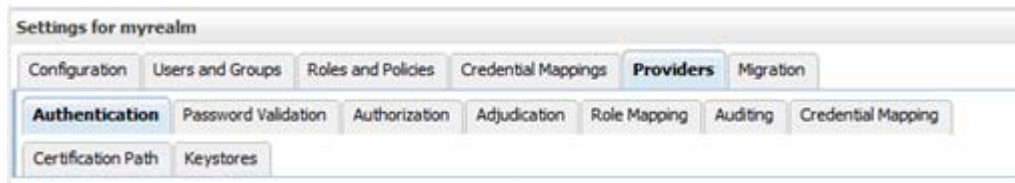
Task 4: Ensure Proper Order of Authentication Providers

Once you have added external authentication providers to the active security realm, use this procedure to define the order in which they are called by WebLogic Server. By default, new authentication providers are added to the bottom of the list and are therefore called last. See "[Authentication Provider Order](#)" on page E-3 for details.

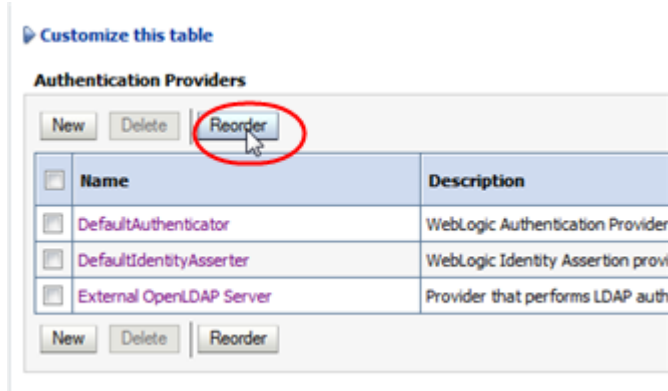
1. If you have not done so already, access the active security realm and lock it for editing. See "[Edit the WebLogic Server Active Security Realm](#)" on page E-5 for instructions.
2. In the Settings for myrealm control bar, select the **Providers** tab.



The **Authentication** secondary tab is selected by default.

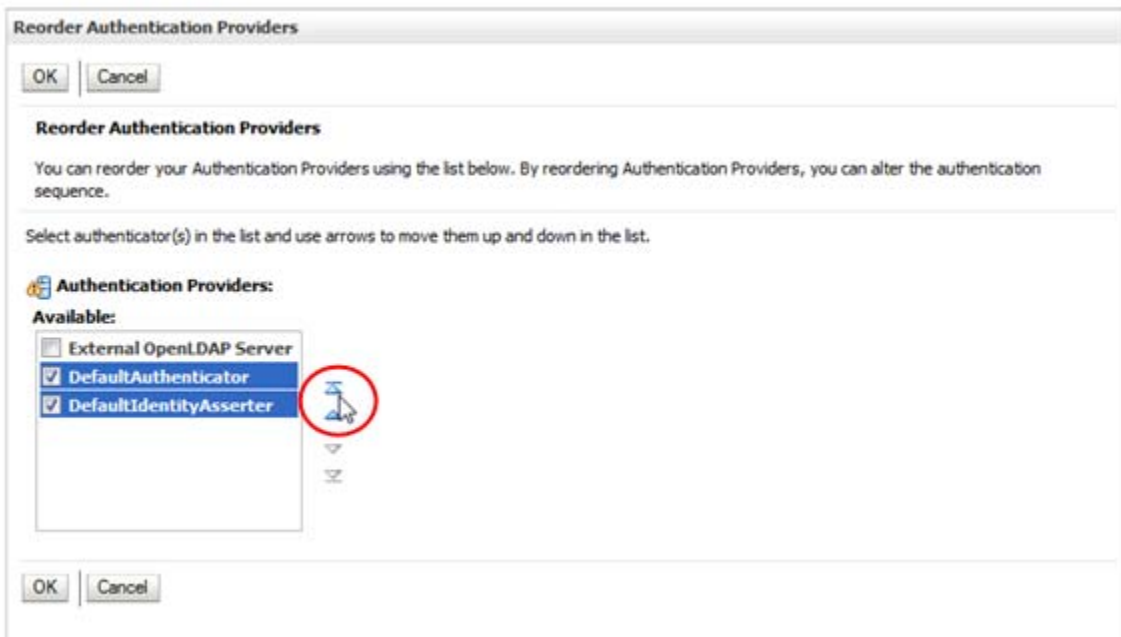


3. In the Authentication Providers table, click **Reorder**.

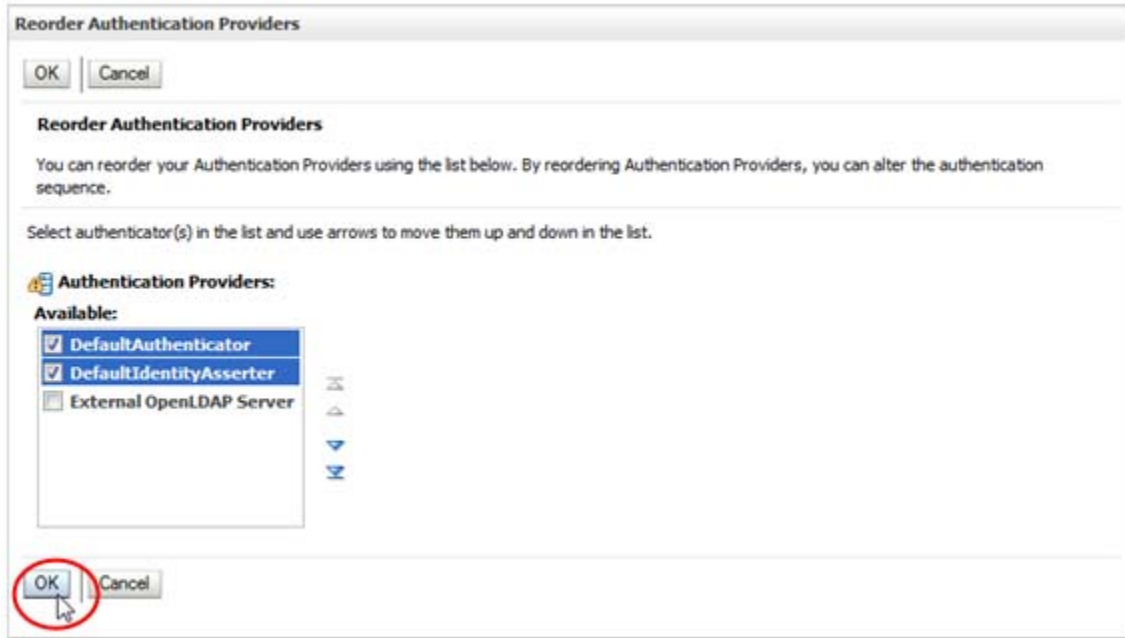


4. In the Reorder Authentication Providers table, arrange the providers in the order you want WebLogic Server to access them, from first to last. Select the check box of the providers you want to reorder, then use the arrow buttons to move them up or down in the list.

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**.



The Authentication Providers table is updated.

Authentication Providers

New Delete Reorder Showing 1 to 4 of 4 Previous | Next

<input type="checkbox"/>	Name	Description	Version
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider	1.0
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
<input type="checkbox"/>	My External OpenLDAP Server	Provider that performs LDAP authentication	1.0
<input type="checkbox"/>	My AD Server	Provider that performs LDAP authentication	1.0

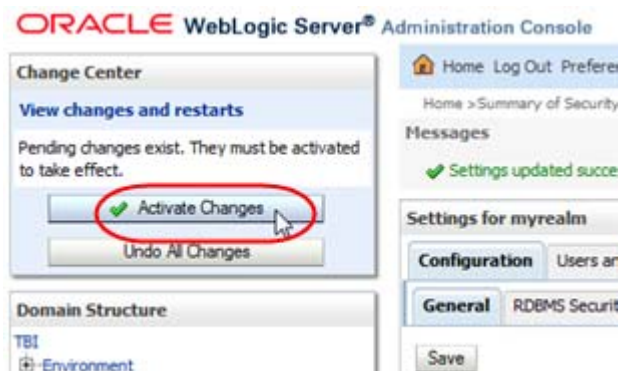
New Delete Reorder Showing 1 to 4 of 4 Previous | Next

6. Proceed to "Task 5: Apply All Configuration Changes" on page E-19.

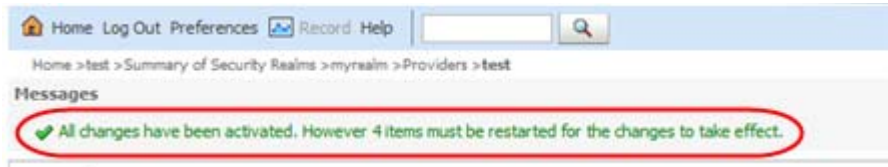
Task 5: Apply All Configuration Changes

Use this procedure to apply all changes you have made during this editing session. The changes are applied to WebLogic Server and STA.

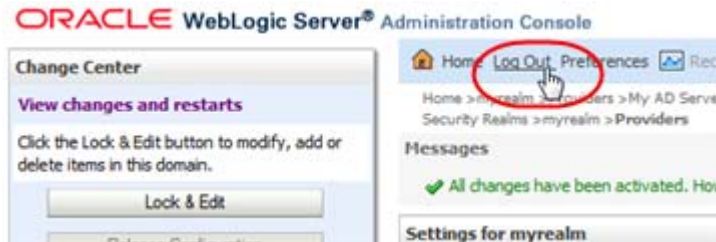
1. In the Change Center section, click **Activate Changes**.



The Messages area indicates that STA must be restarted for the changes to take effect.



2. Log out of the WebLogic Administration console.



3. Open a terminal session on the STA server and log in as the system root user.
4. Stop all STA services. See the *STA Administration Guide* for command usage details.

```
# STA stop all
Stopping the stau service.....
Successfully stopped the stau service
Stopping the staadapter service.....
Successfully stopped the staadapter service
Stopping the staengine service.....
Successfully stopped the staengine service
Stopping the staweblogic service.....
Successfully stopped the staweblogic service
Stopping the staservd Service...
Successfully stopped staservd service
Stopping the mysql service.....
Successfully stopped mysql service
#
```

5. Start all STA services.

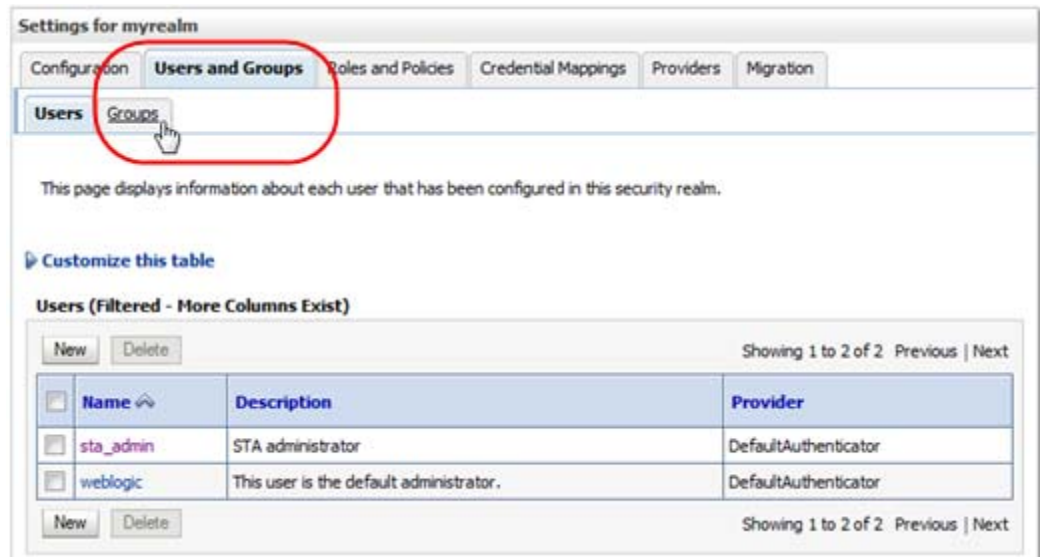
```
# STA start all
Starting mysql Service..
mysql service was successfully started
Starting staservd Service.
staservd service was successfully started
Starting staweblogic service.....
staweblogic service was successfully started
Starting staengine Service.....
staengine service was successfully started
Starting staadapter Service.....
staadapter service was successfully started
Starting stau Service.....
stau service was successfully started
#
```

6. Proceed to ["Verify Configuration of Authentication Providers"](#) on page E-21.

Verify Configuration of Authentication Providers

After you have finished configuring one or more external authentication providers for STA, use this procedure to verify that WebLogic Server can access the appropriate users and groups.

1. If you have not done so already, access the active security realm and lock it for editing. See ["Edit the WebLogic Server Active Security Realm"](#) on page E-5 for instructions.
2. In the Settings for myrealm control bar, select the **Users and Groups** tab and then the **Groups** secondary tab.



The screenshot shows the 'Settings for myrealm' control bar with the 'Users and Groups' tab selected. Below it, the 'Groups' sub-tab is highlighted with a red circle. The main content area shows a table of users with the following data:

Name	Description	Provider
sta_admin	STA administrator	DefaultAuthenticator
weblogic	This user is the default administrator.	DefaultAuthenticator

The Groups screen appears.

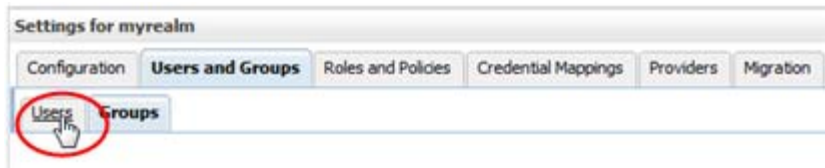
3. Verify that the Groups table includes groups from all configured external authentication providers. The following example shows groups from two external providers.



The screenshot shows the 'Groups' screen with a table of groups. Two rows are circled in red, indicating groups from external providers:

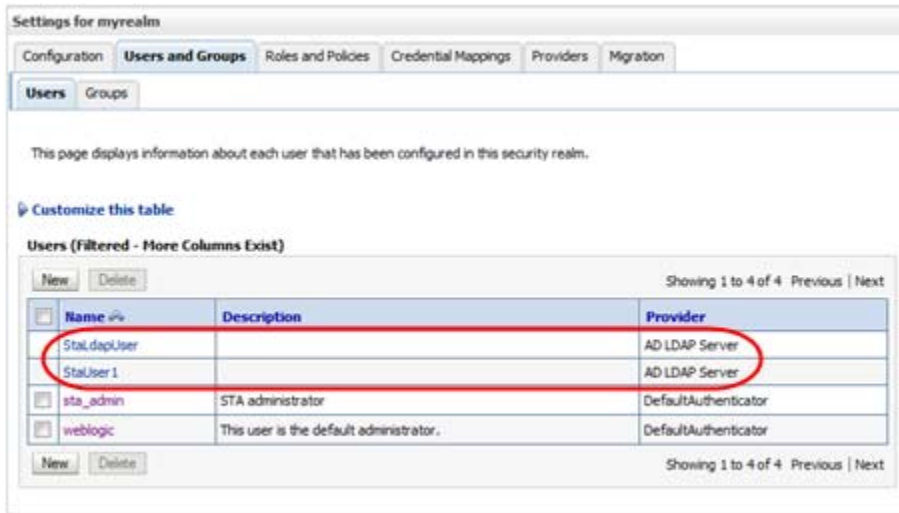
Name	Description	Provider
Administrators	Administrators can view and modify all resource attributes and start and stop servers.	AD LDAP Server
StorageTapeAnalyticsUser	Storage Tape Analytics User Role Group	AD LDAP Server

4. In the Settings for myrealm control bar, select the **Users** secondary tab.

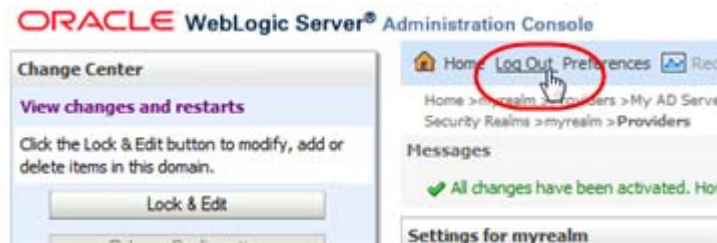


The Users screen appears.

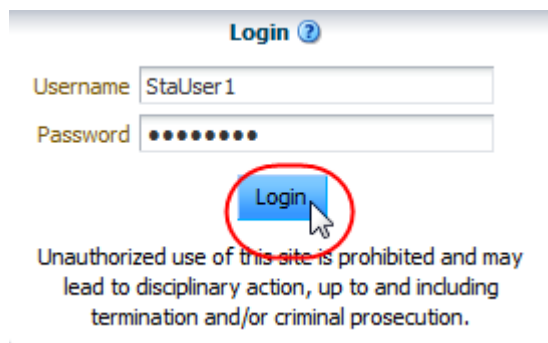
5. Verify that the Users table includes all users assigned to the STA access group (StorageTapeAnalyticsUser) on the configured external providers. The following example shows users from two external providers.

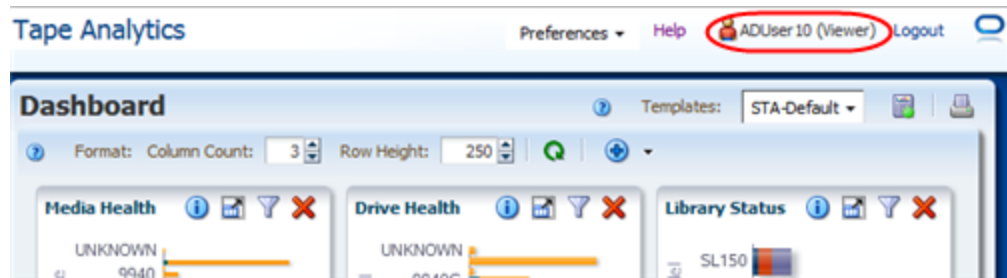


6. Log out of the WebLogic Server Administration console.



7. Verify that you can use a user account from the external authentication provider to log in to STA and display the Dashboard.





8. If a user from an external authentication provider requires STA Operator or Administrator privileges, use the STA user interface to change their role. See the *STA User's Guide* for instructions. See "[Default STA User Role](#)" on page E-3 for additional information.

Tasks for Configuring IBM RACF Authentication Providers

Use the following procedures to configure IBM RACF authentication providers. You must complete the procedures in the order listed.

To configure OpenLDAP and Microsoft Active Directory authentication providers, see "[Tasks for Configuring Active Directory and OpenLDAP Authentication Providers](#)" on page E-4.

- "[Task 1: Review IBM RACF Mainframe Minimum Requirements](#)" on page E-23
- "[Task 2: Enable Mainframe Support for STA RACF Authorization](#)" on page E-23
- "[Task 3: Configure AT-TLS](#)" on page E-24
- "[Task 4: Create the RACF Profiles Used by the CGI Routine](#)" on page E-29
- "[Task 5: Import the Certificate File and Private Key File \(optional\)](#)" on page E-29
- "[Task 6: Test the CGI Routine](#)" on page E-29
- "[Task 7: Set Up RACF/SSP for the WebLogic Console](#)" on page E-30
- "[Task 8: Configure SSL Between STA and RACF](#)" on page E-30
- "[Task 9: Configure the WebLogic Server](#)" on page E-31
- "[Task 10: Install RACF/SSP on the WebLogic Console](#)" on page E-31

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.

Task 1: Review IBM RACF Mainframe Minimum Requirements

See the *STA Requirements Guide* for complete RACF requirements, including required PTFs that must be installed on the MVS system to configure STA authentication with RACF.

Task 2: Enable Mainframe Support for STA RACF Authorization

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.

For STA to use RACF for access authentication, on the MVS system you must set up an SMC Started Task that runs the HTTP server. See the ELS document *Configuring and Managing SMC* for detailed instructions.

Note: 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.

Note: 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.

Task 3: Configure AT-TLS

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 *STA Requirements Guide*.

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

Use this procedure to configure AT-TLS so the port number defined to the SMC HTTP Server and WebLogic is encrypted to the STA server.

1. 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.

2. Configure the Policy Agent (PAGENT)

The Policy Agent address space controls which TCP/IP traffic is encrypted.

- a. 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)
```

- b. 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.

- c. Configure PAGENT.

For example:

```
TTLSSRule TBI-TO-ZOS
{
  LocalAddr localtcpipaddress
  RemoteAddr remotetcpipaddress
  LocalPortRange localportrange
  RemotePortRange remoteportrange
  Jobname HTTPserverJobname
  Direction Inbound
  Priority 255
  TLSGroupActionRef gAct1~TBI_ICSF
  TLSEnvironmentActionRef eAct1~TBI_ICSF
  TLSConnectionActionRef cAct1~TBI_ICSF
}
TLSGroupAction gAct1~TBI_ICSF
{
  TLSEnabled On
  Trace 2
}
TLSEnvironmentAction eAct1~TBI_ICSF
{
  HandshakeRole Server
  EnvironmentUserInstance 0
  TLSKeyringParmsRef keyR~ZOS
}
TLSConnectionAction cAct1~TBI_ICSF
{
  HandshakeRole ServerWithClientAuth
  TLSCipherParmsRef cipher1~AT-TLS__Gold
```

```

TTLSTransactionAdvancedParmsRef cAdv1~TBI_ICSF
  CtraceClearText Off
  Trace 2
}
TTLSTransactionAdvancedParms cAdv1~TBI_ICSF
{
  ApplicationControlled Off
  HandshakeTimeout 10
  ResetCipherTimer 0
  CertificateLabel certificatelabel
  SecondaryMap Off
}
TTLSTransactionParms keyR~ZOS
{
  Keyring keyringname
}
TTLSTransactionCipherParms 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

3. Activate RACF Classes. Either the RACF panels or the CLI can be used.

The RACF classes include:

- DIGTCERT
- DIGTNMAP
- DIGTRING

SERVAUTH class must be RAACLISTed to prevent PORTMAP and RXSERV from abending.

```

SETROPTS RAACLIST(SERVAUTH)
RDEFINE SERVAUTH **UACC(ALTER) OWNER (ACFADM)
RDEFINE STARTED PAGENT*.* OWNER (ACFADM) STDATA(USER(TCPIP) GROUP(STCGROUP)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE) OWNER (ACFADM)
RDEFINE FACILITY IRR.DIGTCERT.LIST UACC(NONE) OWNER (ACFADM)
RDEFINE FACILITY IRR.DIGTCERT.GENCERT UACC(NONE) OWNER (ACFADM)

```

4. Define RACF Keyrings and Certificates

- a. 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

```
RACDCERT ID(stcuser) GENCERT CERTAUTH SUBJECTSDN(CN('serverdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('calabel') TRUST
SIZE(1024) KEYUSAGE (HANDSHAKE, DATAENCRYPT, CERTSIGN)
```

Note: This is the CA certificate for the STA system.

where:

- * *stcuser*: RACF user id associated with the TCPIP address space
- * *serverdomainname*: Domain name of the z/OS server (for example, MVSA.COMPANY.COM)
- * *companyname*: Organization name
- * *unitname*: Organizational unit name
- * *country*: Country
- * *calabel*: Label for certificate authority (for example, CATBISERVER)

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('serverdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('serverlabel')
TRUST SIZE(1024) SIGNWITH(CERTAUTH LABEL('calabel'))
```

Note: This is the SERVER certificate.

where:

- * *stcuser*: RACF user id associated with the TCPIP address space
- * *serverdomainname*: Domain name of the z/OS server (for example, MVSA.COMPANY.COM)
- * *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

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('clientdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('clientlabel')
TRUST SIZE(1024) SIGNWITH(CERTAUTH LABEL('calabel'))
```

Note: This is the CLIENT certificate.

where:

- * *stcuser*: RACF user id associated with the TCPIP address space

- * *clientdomainname*: Domain name of the STA client (for example, TBIA.COMPANY.COM)
- * *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.

b. Connect the CA, SERVER, and CLIENT certificates to the keyring specified in the PAGENT configuration:

```
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('keyringname') DEFAULT USAGE(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('keyringname') USAGE(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

c. 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.

Task 4: 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.

Task 5: Import the Certificate File and Private Key File (optional)

Use this procedure to 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.

Task 6: Test the CGI Routine

Use this procedure to test the CGI routine from a browser.

1. 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&r

```
oles=StorageTapeAnalyticsUser
```

The resulting output indicates whether or not 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.

Task 7: 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.

Use this procedure to place the RACF SSP in the proper location, if it has not been already.

1. 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.

Task 8: Configure SSL Between STA and RACF

Use this procedure to install the MVS security certificate on the STA server and import it into the system-wide 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 "[Task 1: Review IBM RACF Mainframe Minimum Requirements](#)" on page E-23 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 system-wide 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 system-wide Java keystore.
- -storetype indicates the type of keystore.

Task 9: Configure the WebLogic Server

To configure WebLogic for RACF authentication, use the procedure in "[Reconfigure WebLogic to use a Different Security Certificate](#)" on page D-2.

Task 10: Install RACF/SSP on the WebLogic Console

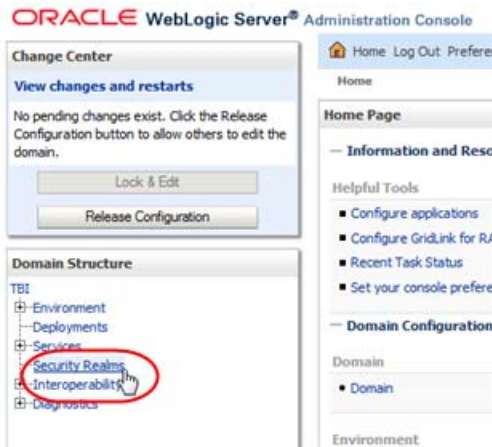
1. Go to the WebLogic console login screen using the HTTP (STA 2.1.x default is 7019) or HTTPS (STA 2.1.x default is 7020) port number you selected during STA installation.

```
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**.



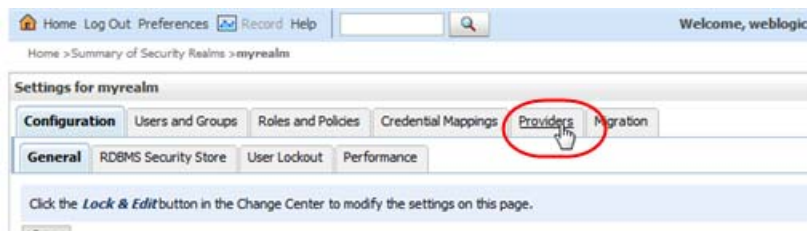
4. In the Realms section, select the **myrealm** active link (select the name itself, not the check box).



5. In the Change Center section, click **Lock & Edit**.



6. Select the **Providers** tab.



7. In the Authentication Providers section, click **New**.



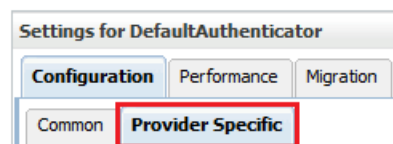
8. Enter the name of the authentication provider you want to add (for example, STA RacfAuthenticator), and select RacfAuthenticator in the **Type** menu. Click **OK**.

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).

<input type="checkbox"/>	Name
<input type="checkbox"/>	DefaultAuthenticator
<input type="checkbox"/>	DefaultIdentityAsserter
<input type="checkbox"/>	RacfAuthenticator

11. In the **Control Flag** menu, select Sufficient, and then click **Save**.
12. Click the **Provider Specific** tab, and then click **Save**.



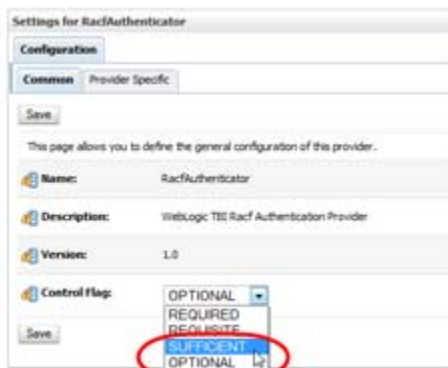
13. Click the **Providers** locator link to return to the Authentication Providers screen.



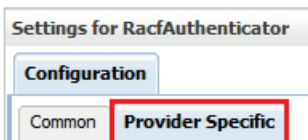
14. In the Authentication Providers table, select the RACF authenticator name you created in Step 8 (select the name itself, not the check box).

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider
<input type="checkbox"/>	RacAuthenticator	WebLogic TBI Racf Authentication Provider

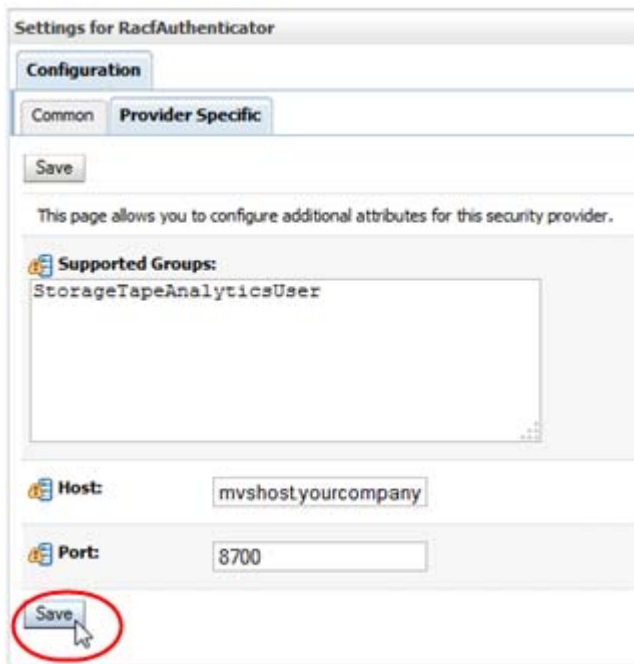
15. In the **Control Flag** menu, select Sufficient, and then click **Save**.



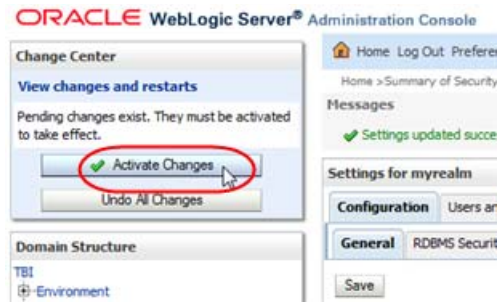
16. Click the **Provider Specific** tab.



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
```

Configuring SNMP v2c Mode

This appendix includes the following sections:

- [When to Use SNMP v2c Mode](#)
- [SNMP v2c Mode Configuration Process](#)
- [SNMP v2c Configuration Tasks](#)

When to Use SNMP v2c Mode

For optimal SNMP security, Oracle recommends using the SNMP v3 protocol for communication between STA and the libraries. See "[Understanding Library SNMP Configuration for STA](#)" on page 5-1 for details.

The SNMP v2c protocol is less secure than SNMP v3 and by default is not enabled on STA. However, if SNMP v3 communication is not possible—for instance, SNMP v3 is not configured on a library that STA will be monitoring—you can enable and configure SNMP v2c mode for STA.

The SNMP v3 configuration process is described in [Chapter 5, "Configuring SNMP on the Libraries"](#) and [Chapter 6, "Configuring Library Connections in STA"](#). This appendix describes the procedures that differ for SNMP v2c configuration.

SNMP v2c Mode Configuration Process

The process for configuring the libraries and STA to use SNMP v2c for SNMP communications is as follows:

1. In [Chapter 5](#), follow all procedures shown in [Table 5–1, "Tasks to Configure Libraries for STA"](#), except:
 - Replace "[Create the STA SNMP v3 Trap Recipient](#)" with "[Create the STA SNMP v2c Trap Recipient on the Library](#)" on page F-2.
 - After completing the process in [Table 5–1](#), perform "[Enable SNMP v2c Mode for STA](#)" on page F-3.
2. Configure SNMP v2c in STA. See [Chapter 6, "Configuring Library Connections in STA"](#) for instructions.

SNMP v2c Configuration Tasks

- "[Create the STA SNMP v2c Trap Recipient on the Library](#)" on page F-2
- "[Enable SNMP v2c Mode for STA](#)" on page F-3

Create the STA SNMP v2c Trap Recipient on the Library

Use this procedure to define the STA server as an authorized recipient of SNMP v2c traps and to define traps the library sends. Depending on library model, you can use the library CLI, SL Console, or SL150 browser interface.

Notes:

- Separate trap levels with commas.
 - 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`.
 - Oracle recommends *not* using the values "public" or "private" for the community string, as these values are well known and present a security risk. See "[SNMP v2c Community String](#)" on page 5-2 for additional requirements.
-
-

Using the library CLI (all libraries except SL150)

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

```
> 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 stasmp
```

```
request Id
request Id 2
Device 1,0,0,0
Success true
Done
```

```
Failure Count 0
Success Count 1
```

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

```
> snmp listTrapRecipients
```

```
requestId
requestId 3
```

```
Attributes Community stasmp
Host 192.0.2.20
```

Index 1
 Port 162
 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

Using the SL Console (SL500 libraries only)

1. Use the SL Console to log in to the library.
2. From the **Tools** menu, select **System Detail**.
3. In the navigation tree, select **Library**.
4. Select the **SNMP** tab and then the **Add Trap Recipients** tab.
5. Complete the screen as follows:
 - Host: IP address of the STA server.
 - TrapLevel: 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 – Specify the SNMP v2c trap community string (for example stasnp).
6. Click **Apply** to add the trap recipient.

Using the SL150 user interface

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, stasnp).
6. Click **OK** to add the trap recipient.

Enable SNMP v2c Mode for STA

By default, SNMP v2c is disabled on STA. Use this procedure to enable it.

1. Establish a terminal session with the STA server and log in as the system root user.
2. 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.

3. Edit the SNMP version properties file.

```
# vi TbiSnmpVersionSupport.properties
```

4. Change the SNMP v2c parameter to true.

```
V2c=true
```

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

```
# STA stop all
```

```
# STA start all
```

C

changing SNMP client attributes, 6-4
client attributes, 6-4
complex IDs, 4-3

D

deinstalling, 9-1

F

firewall port configuration, 3-4

L

LDAP configuration, E-8
library configuration, 5-1
 complex IDs, 4-3
 Dual TCP/IP, 4-2
 optional configuration script, 4-6
 Redundant Electronics, 4-2
 SL500 fast load, 4-5
 SNMP configuration, 5-1
 SNMP worksheet, C-5
 tasks, 4-6
 user interfaces, 4-5
 volume label formatting, 4-4
Linux installation
 overview, 2-1
 post-installation tasks, 2-7
 preparation tasks, 2-2
 tasks, 2-4
Linux PATH setting, 7-2

R

RACF configuration, E-23
reinstalling, 9-1, 9-3

S

service requests, 1-5
SNMP
 confirm connectivity, 6-2
 management
 add trap recipient, 8-25

change client attributes, 6-4

SSP

configuration, E-1
configure RACF, E-23
configure WebLogic Open LDAP, E-8

STA

download, 3-11

STA configuration

certificates, D-1
 establish initial connection, D-1
 reconfigure WebLogic, D-2
 replace Oracle certificate, D-9

services, 7-1

resource monitor, 7-1

restart services daemon, 7-2

update Linux PATH setting, 7-2

verify library connectivity, 7-2

SNMP, 6-1

STA database backup service, 7-1

tasks, 6-1

STA installation

console installer, 3-16

general prerequisites, 3-9

graphical installer, 3-16

overview, 3-1

steps to install, 3-16

STA server

port configuration, 3-4

T

trap recipients

adding, 8-25

U

upgrading STA, 8-1

user accounts

 MySQL requirements, 3-3

 WebLogic requirements, 3-3

V

v2c mode

configuration process, F-1

create trap recipient, F-2

enable, F-3
overview, F-1
volume label formatting, 4-4
volume serial numbers, duplicate, 4-5