# StorageTek Tape Analytics

## Configuration Guide

Version 1.0.2

Part Number: E28378-04
April 2013

Submit comments about this document to STP_FEEDBACK_US@ORACLE.COM.

StorageTek Tape Analytics Configuration Guide

E28378-04

Oracle welcomes your comments and suggestions for improving this book. Contact us at STP_FEEDBACK_US@ORACLE.COM. Please include the title, part number, issue date, and revision.

# Table of Contents

**Summary of Changes** ........ 7

v1.0.2 Revision, April 2013 ........ 7

v1.0.2, December 2012 ........ 7

v1.0.1, July 2012 ........ 8

v1.0.0, April 2012 ........ 8

**Preface** ........ 11

STA Documentation ........ 11

Access to Oracle Support ........ 11

**1 Configuring the Libraries for STA** ........ 13

Library Configuration Concepts ........ 14

Library User Interfaces ........ 14

SNMP Configuration for STA ........ 17

Support for Dual TCP/IP and Redundant Electronics ........ 19

Drive ADI Interface ........ 21

Volume Label Formatting ........ 23

Drive Cleaning Warning ........ 24

Library Complex IDs ........ 25

Library Configuration Process ........ 26

Determine Configuration Parameters ........ 27

Log In to the Library ........ 30

Verify the Library Firmware Version ........ 34

Retrieve the Library IP Address ........ 36

Verify the Drive Controller Card Version ........ 41

Enable ADI on the Library ........ 43

Enable SNMP on the Library ........ 46

Ensure an SNMP v2c User ........ 49

Create an SNMP v3 User ........ 55

Retrieve the Library SNMP Engine ID ........ 60

Create an SNMP v3 Trap Recipient ........ 61

Set the SL500 Volume Label Format ........ 68

Set the SL150 Volume Label Format ........ 70

Set the Drive Cleaning Warning ........ 71

Ensure the Correct Library Complex ID ........ 72

2 Configuring SNMP in the STA Application ........ 75
Configuration Process ........ 75
Verify SNMP Communications With the Library ........ 76
Log In to the STA User Interface ........ 78
Configure SNMP Client Settings for STA ........ 80
Configure SNMP Connections With the Library ........ 84
Verify the Library is Operational ........ 87
Test the SNMP Connection to the Library ........ 89
Get the Latest Configuration Data From the Library ........ 91
Configuration Troubleshooting ........ 93
Troubleshoot an Unsuccessful SNMP Connection ........ 93
Troubleshoot Unsuccessful Trap Processing ........ 96
3 Configuring Email Notifications ........ 99
How Email Notifications Work ........ 100
Message Types ........ 101
Test Message ........ 101
Drive Message ........ 101
CAP Message ........ 101
PTP Message ........ 101
Library Message ........ 101
Email Tasks ........ 102
Define SMTP Server Details ........ 102
Add an Email Address ........ 105
Test your SMTP and Email Address Setup ........ 106
Edit an Email Address ........ 106
Delete an Email Address ........ 107
4 Configuring STA Services ........ 109
Preparation Task ........ 110
Optional: Update Linux PATH Setting ........ 110
Backup Configuration Tasks ........ 111
Review the staservadm Utility Preferences ........111
Determine STA Backup Preferences ........ 112
Configure the Remote Backup Server ........ 113
Configure the STA Backup Service ........ 114
Resource Monitor Configuration Tasks ........ 117
Review the staresmonadm Utility Preferences ........ 117
Determine STA Resource Monitor Preferences ........ 119
Configure the STA Resource Monitor ........ 120
Services Daemon Task ........ 123
Restart the STA Services Daemon (optional) ........ 123
5 Configuring STA Identity Management - Local Users and Open LDAP ........ 125
STA Roles ........ 125
STA Role Assignment ........ 125
Configure WebLogic Local Users ........ 126
Configure WebLogic Open LDAP Users ........ 131
6 Configuring STA Identity Management - RACF ........ 141
IBM RACF Mainframe Minimum Requirements........ 142

Installing and Configuring STA's RACF Authorization Facility ............ 142
Enable Mainframe Support for STA RACF Authorization ............ 142
Configure AT-TLS ............ 143
Create the RACF Profiles ............ 152
Import the Certificate File and Private Key File ............ 153
Test the CGI Routine ............ 158
Set Up RACF/SSP for the WebLogic Console ............ 159
Configure SSL Between STA and RACF ............ 160
Configure the WebLogic Server ............ 161
Install RACF/SSP on the WebLogic Console ............ 171

7 Configuring Certificates ............ 181

Oracle Certificate ............ 181
Establishing the Initial HTTPS/SSL Connection ............ 182
Reconfigure the WebLogic Server to use a Different Security Certificate ............ 187
Replace the Oracle Certificate ............ 194

A Configuring SNMP v2c Mode ............ 197

SNMP v2c Mode Configuration Process ............ 197
Create an SNMP v2c Trap Recipient ............ 198
Enable SNMP v2c Mode for STA ............ 203

Index ............ 205

# Summary of Changes

## v1.0.2 Revision, April 2013

Document update ONLY — The STA 1.0.2 version of this document was revised with the following changes. These updates are flagged with change bars in the margin.

- Updates to Chapter 1, "Configuring the Libraries for STA":
    - "Drive ADI Interface" — Added support for HP LTO-6 drives; added detail that configuring firmware on an IBM LTO-5 or LTO-6 drive is performed with Virtual Operator Panel (VOP), and to contact Oracle support for assistance.

## v1.0.2, December 2012

The following sections were updated for this release. These updates are flagged with change bars in the margin. Minor updates are not listed.

- Updates to Chapter 1, "Configuring the Libraries for STA":
    - Multiple sections — Added SL150 configuration content.
    - "Drive ADI Interface" — Added LTO-6 drive information.
    - "Volume Label Formatting" — Added label orientation content for SL500.
    - "Library Configuration Process" — Added table of library configuration steps.
    - "Ensure an SNMP v2c User" — Added new information as to when a v2c user is required. Also changed command requirement: When adding a v2c user, *community_name* can be "public", or another name of your choice.
    - "Set the SL500 Volume Label Format" — Added new procedure to set the host label orientation.
- Updates to Chapter 2, "Configuring SNMP in the STA Application":
    - Multiple sections — Added SL150 content.
    - "Configure SNMP Client Settings for STA" — Added new information concerning what fields must be filled out in relation to a library's SNMP protocol version. Also added definitions for two new fields applicable only to the v2c protocol, User Community and Trap Community.

- “Troubleshoot Unsuccessful Trap Processing” — Added two additional troubleshooting steps.
- Updates to Appendix A, “Configuring SNMP v2c Mode”:
  - Added new information as to when to enable v2c mode.
  - “SNMP v2c Mode Configuration Process” — Section simplified.
  - “Create an SNMP v2c Trap Recipient” — Changed command requirement: When adding a v2c trap recipient, *community_name* can be “public”, or another name of your choice.

# v1.0.1, July 2012

The following sections were updated for this release.

- Updates to Chapter 1, “Configuring the Libraries for STA”:
  - “Drive ADI Interface” — Added additional information on enabling ADI on IBM drives.
  - “Volume Label Formatting” — Added Caution statement addressing the consequences of not enabling STA mode.
  - “Library Complex IDs” — Added Caution information about complex ID settings affecting SDP.
  - “Set the SL500 Volume Label Format” — Added Caution statement addressing the consequences of not enabling STA mode.
  - “Ensure the Correct Library Complex ID” — Added Caution information about complex ID settings affecting SDP.
- Updates to Chapter 2, “Configuring SNMP in the STA Application”:
  - “Configuration Troubleshooting” — New section. Existing troubleshooting content moved to this section.
  - “Troubleshoot an Unsuccessful SNMP Connection” — Added information on using **`traceroute`** command.
- Updates to Chapter 3, “Configuring Email Notifications”:
  - “How Email Notifications Work” — Added Note about temporarily disabling notifications when bringing a library offline and online.
  - “Define SMTP Server Details” — Added Note, “If the email server does not require authentication, you may need to specify localhost for the SMTP Host Address.”
- Updates to Chapter 4, “Configuring STA Services”:
  - “Optional: Update Linux PATH Setting” — Clarified that this procedure is optional. Content also re-written.

# v1.0.0, April 2012

Initial release.

v1.0.0, April 2012

v1.0.0, April 2012

# Preface

This document describes configuring Oracle's StorageTek Tape Analytics (STA) product. Before reading this book, you should have already planned for and installed STA as described in the *StorageTek Tape Analytics Planning and Installation Guide.*

## STA Documentation

| Document Title | Description |
|---|---|
| *StorageTek Tape Analytics Release Notes* | Read this document before installing and using STA. It contains important release information, including known issues. |
| *StorageTek Tape Analytics Planning and Installation Guide* | Use this book to plan for installation of STA, install the Linux platform, and install the STA software. |
| *StorageTek Tape Analytics Configuration Guide* | After installing the STA software, use this book to configure libraries, SNMP, email notification, services, identity management, and certificates. |
| *StorageTek Tape Analytics Administration Reference Guide* | Use this book to learn about STA administrative tasks, including server, services, and password administration. |
| *StorageTek Tape Analytics User Interface Guide* | Use this book to learn about the STA user interface. It describes the layout of screens and provides step-by-step instructions for modifying their display so you can tailor them to your needs. |
| *StorageTek Tape Analytics Data Reference Guide* | Use this book to learn about using and interpreting the data displayed by STA. It provides definitions for all library, drive, and media data fields displayed by STA. It also provides reference information for all STA toolbars and data input fields. |
| *StorageTek Tape Analytics Security Guide* | Read this document for important STA security information, including requirements, recommendations, and general security principles. |

## Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support:

http://www.oracle.com/support/contact.html

http://www.oracle.com/accessibility/support.html (for hearing impaired)

# 1

# Configuring the Libraries for STA

This chapter describes the process for configuring all library models to enable them to send the proper data to StorageTek Tape Analytics (STA). This chapter includes the following topics:

- "Library Configuration Concepts" on page 14
- "Library Configuration Process" on page 26

# Library Configuration Concepts

This section includes the following topics:

- "Library User Interfaces" on page 14
- "SNMP Configuration for STA" on page 17
- "Support for Dual TCP/IP and Redundant Electronics" on page 19
- "Drive ADI Interface" on page 21
- "Volume Label Formatting" on page 23
- "Drive Cleaning Warning" on page 24
- "Library Complex IDs" on page 25

## Library User Interfaces

The SL500, SL3000, and SL8500 have both a command line interface (CLI) and a graphical user interface, called the StorageTek Library Console (SL Console). The SL150 exclusively uses a browser-based user interface.

Each procedure in this chapter identifies which interface to use; in some cases, you can choose which to use.

- "Using the CLI (all libraries except SL150)" on page 14
- "Using the SL Console (all libraries except SL150)" on page 15
- "Using the SL150 User Interface" on page 16

### Using the CLI (all libraries except SL150)

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.

> **Note –** The SL150 does not have a customer-accessible CLI interface. This library is configured exclusively with its browser-based user interface.

Most CLI examples in this chapter 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 in the examples. Examples are provided whenever there are significant differences.

You can use the following optional script to display the library CLI commands. It will step you through the library configuration process, request data to be entered, and then display the commands that can be copied and pasted into the library CLI.

```
/Oracle/StorageTek_Tape_Analytics/common/bin/STA-lib-config-steps.sh
```

> **Note –** Execute the script using the **sh** command. Be sure to read and understand the library configuration steps in this chapter before executing the script.

### *CLI Usage Tips*

- Use a terminal emulator, such as PuTTY, to establish an SSH (secure shell) connection to the library CLI.
- You may also want to enable logging for your terminal session. This will allow you to review your activity, should you need to troubleshoot errors.
- For the SL500, library commands are case-sensitive; for SL3000 and SL8500, they are not.
- Because some of the commands are quite long, reduce the text font size and stretch the width of the terminal window.
- With some firmware versions, the CLI times out after six hours.
- For complex commands, you may want to type the command in a text file on your PC or workstation, and then copy and paste the command directly into the CLI command line. This will help to reduce typing errors in the CLI. If you are using PuTTY, you can paste text by right-clicking in the terminal window.

  You may find this method especially helpful for the following procedures:

  - "Create an SNMP v3 User" on page 55
  - "Create an SNMP v3 Trap Recipient" on page 61
- 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.
- To display Help for any CLI command, type "help" plus the command name; for example, "help snmp". The Help function displays command syntax and valid entries and characters for selected attributes.

## Using the SL Console (all libraries except SL150)

To log in with the SL Console, you must use a PC or workstation on which either the Standalone SL Console or the Web-based SL Console has been installed. See your storage administrator or the library *User's Guide* for details.

Before using the SL Console, you need to verify that the version you are using meets the STA minimum requirements. For details, see the "Pre-Installation Planning" chapter within the *StorageTek Tape Analytics Planning and Installation Guide*.

## Using the SL150 User Interface

The SL150 is configured exclusively with its browser-based user interface. The user interface is a web application, so there is nothing to install on user workstations. Once you have set up the library's network interface, you enter the library's hostname or IP address into a standards-compliant web browser, such as Mozilla Firefox, and log in.

## SNMP Configuration for STA

**Note –** SNMP v3 is the recommended protocol for SNMP communications between STA and the libraries. Depending on your site requirements, however, you may choose to use v2c. This section describes the recommended v3 configuration. See Appendix A, "Configuring SNMP v2c Mode" on page 197 for information on configuring the v2c protocol.

Communication between the STA server and the libraries it monitors is done through the SNMP interface. The libraries send data to STA through SNMP traps, and STA retrieves library configuration data through SNMP get functions.

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

To set up communication between the STA server and the libraries, you must perform some configuration procedures on the libraries and some on the STA server. This chapter describes the procedures you must perform on the libraries. See Chapter 2, Configuring SNMP in the STA Application" on page 13 for the procedures you must perform on the STA server.

### SNMP Communication

STA uses the v3 SNMP protocol to communicate with the library; however, in some cases, the initial communication handshake between a library and the STA server is done through the v2c protocol. Refer to "Ensure an SNMP v2c User" on page 49 to see if a v2c user is required for your library for the initial handshake.

The traps and get functions are done through the v3 protocol. The authentication, encryption, and message integrity features in SNMP v3 provide a secure mechanism for sending library data.

To set up SNMP v3 communication on each library, you define the library as a v3 user and the STA server as a 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).

### Unique v3 User

STA supports one and only one SNMP v3 library user. Therefore, the same v3 user must be defined on all libraries monitored by a single STA server. Your libraries may already have one or more v3 users, and you can use one of these for STA communication. However, it is highly recommended that you set up a new, unique v3 user for this purpose. See "Create an SNMP v3 User" on page 55 for detailed instructions.

### SNMP Engine IDs

The SNMP v3 protocol requires each SNMP device to have a globally unique engine ID. Therefore, the STA server and the libraries each have their own unique 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.**

According to the SNMP protocol, 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.

See "Create an SNMP v3 User" on page 55 and "Create an SNMP v3 Trap Recipient" on page 61 for detailed instructions.

## Support for Dual TCP/IP and Redundant Electronics

**Note –** This section is applicable only to SL3000 and SL8500 libraries.

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.

### Library IP Addresses for 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, review the following section, "Configuring the STA Connection to Support These Features", to determine what is supported by STA.

### Configuring the STA Connection to Support These Features

STA is capable of maintaining uninterrupted connections with 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. In addition, 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, it is recommended 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, it will maintain a connection with the library in the event of a port failover.

If STA is configured to support Redundant Electronics, it will maintain a connection with the library in the event of a controller card switch. After a Redundant Electronics switch completes, you must perform a connection test and a data collection in order to verify the library connection and retrieve current library configuration data. See "Managing Library Connections" in the *STA Data Reference Guide* for details.

TABLE 1-1 summarizes the recommended library IP addresses to use when configuring the STA connection to the library.

**TABLE 1-1** Recommended Library IP Addresses for STA Connection

| Activated Features | Primary Library IP | Secondary Library IP |
|---|---|---|
| Neither | 2B port | N/A |
| Dual TCP/IP only | 2B port | 2A port |
| Redundant Electronics only | active card 2B port | standby card 2B port |
| Both[1] | (see footnote) | (see footnote) |

[1] Choose between either the Redundant Electronics or Dual TCP/IP configurations detailed above. The Redundant Electronics configuration is recommended.

## Additional Configuration Considerations for Dual TCP/IP and Redundant Electronics

- For proper use of dual TCP/IP ports, the library ports/interface may require policy routing. For more information, consult the SL3000 or SL8500 *Host Connectivity Guide*.
- When configuring STA with a library that has both Redundant Electronics and Dual TCP/IP support, the network interface subnet on the server on which STA is installed must not be the same as the subnet for the library interface port that is NOT configured for STA use (in the STA GUI “Define Library Connections Details” dialog box). Otherwise, the library may try to send information through those ports (which are unknown to STA), and it will be rejected by STA.
- Make sure your default gateway is the 2B interface.
- If you need assistance with Dual TCP/IP or Redundant Electronics configuration, contact Oracle Support.

## Related Information

See the following topics for additional details:

- For instructions on gathering the appropriate IP addresses from the library, see “Retrieve the Library IP Address” on page 36.
- For instructions on specifying a second STA trap recipient on the library so that STA can support the Dual TCP/IP feature, see “Create an SNMP v3 Trap Recipient” on page 61.
- For instructions on configuring the library connection on the STA server, see “Configure SNMP Connections With the Library” on page 84.

In addition, consult your network administrator and Oracle support representative to ensure the proper network configuration.

# Drive ADI Interface

Oracle's StorageTek modular libraries support LTO (Linear Tape Open) drives from HP and IBM. For a library to send rich LTO drive data to STA, ADI (Automation/ Drive Interface) must be enabled on both the library and the LTO drives. If ADI is not enabled on both, the library will only send minimal data about the LTO drives.

## Enabling ADI on the Drives

The ADI interface is available on the following drive models:

- HP LTO-3, LTO-4, LTO-5, LTO-6
- IBM LTO-3, LTO-4 without the IBM Belisarius adapter card
- IBM LTO-4, LTO-5, LTO-6 with the IBM Belisarius adapter card

**Note –** For all HP LTO drives, after you enable ADI mode in the library, the drive auto-switches to ADI mode on next initialization (library reboot).

**Note –** The Belisarius card provides the interface between the drive and Oracle's Key Manager (OKM) tape encryption solution.

**Note –** If ADI has been enabled on IBM LTO drives, the drives will not be recognized unless 1) ADI has also been enabled on the library, and 2) the library has been rebooted after enabling ADI on the library. See "Enabling ADI on the Library" on page 22.

**Note –** See the "Tape Drive Requirements" section within the *STA Planning and Installation Guide* for LTO drive support information.

The method for enabling ADI on the drives depends on the drive model and manufacturer. See TABLE 1-2 for details.

**TABLE 1-2** How ADI is Enabled on LTO Drives

| Manufacturer/Model | LTO-3 | LTO-4 | LTO-5, LTO-6 |
|---|---|---|---|
| **HP** | Auto-enabled | Auto-enabled | Auto-enabled |
| **IBM without the Belisarius adapter card** | An Oracle support representative must configure the drive hardware for ADI mode. | An Oracle support representative must configure the drive hardware for ADI mode. | Not available |
| **IBM with the Belisarius adapter card**[1] | Not available | An Oracle support representative must configure the drive hardware for ADI mode.<br>Drive and Belisarius card firmware must also meet minimum requirements for STA. | The drive firmware must be configured for ADI mode.[2]<br>Drive and Belisarius card firmware must also meet minimum requirements for STA. |

[1] See the *STA Planning and Installation Guide* for firmware requirements for IBM LTO-4, LTO-5, and LTO-6 drives with the Belisarius adapter card.

[2] This is performed 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 your Oracle support representative must enable ADI manually. Because enabling ADI requires a reboot of the library, it is recommended that you enable ADI now if you plan to include LTO drives in the library in the near future.

**Note –** ADI is enabled by default on the SL150 library.

See “Enable ADI on the Library” on page 43 for instructions on checking the library ADI status and enabling ADI.

For SL3000 and SL8500 libraries, ADI can be enabled only if the library has a high-memory drive controller (HBT) card. If the library has a low-memory HBT card, the ADI interface will not enable successfully. See “Verify the Drive Controller Card Version” on page 41 for instructions.

## Volume Label Formatting

**Note –** This section is applicable only to SL500 and SL150 libraries.

Volume Serial Numbers (VSNs) in SNMP data must be formatted properly for STA to correctly process library exchange data.

- For all SL500 libraries monitored by STA, the label orientation for the host must be set to "left6" and "STA mode" must be set to "on".

  **Note –** "STA mode" affects only the format of the VSN sent to the STA server through SNMP, not the format used on the SL500 library itself.

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

  **Caution –** If these parameters are not set properly, VSNs will be formatted incorrectly for STA. This will cause 1) exchanges processing to be blocked, 2) superfluous attempts by STA to get the latest media data from the library, and 3) irreversible, eight-character VSN records to appear on the Media - Overview screen whenever the "Show Removed Media" preference is set.

For all StorageTek libraries, the media VSN includes a two-character suffix that indicates the media type. For example, a cartridge VSN of "ABC123L4" breaks down as follows:

- The first six characters, "ABC123", are the unique identifier for the media.
- The last two characters, "L4", indicate the media type, in this case LTO4.

For STA reporting to work correctly, the suffix must be excluded. To ensure the proper format:

- For SL500 libraries, see "Set the SL500 Volume Label Format" on page 68
- For SL150 libraries, see "Set the SL150 Volume Label Format" on page 70

## Drive Cleaning Warning

**Note –** This section is applicable only to SL3000 and SL8500 libraries.

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

When the flag is set to “on”, each drive will show a warning health status whenever it needs cleaning. This will also cause 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 will not be affected by the need for cleaning. Therefore, the library top-level status in STA will not be 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 one of them needs cleaning.

See “Set the Drive Cleaning Warning” on page 71 for detailed instructions.

## Library Complex IDs

**Note –** This section is applicable only to SL8500 libraries.

In order 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, so you must ensure they are set correctly:

- Each standalone SL8500 is considered to be a separate complex and therefore must have a unique complex ID.
- Each multi-library complex must have a unique complex ID, and all libraries within the complex must share the same ID.

**Caution –** The Oracle Service Delivery Platform (SDP) also uses complex IDs for tracking library data. If SDP is in use at your site, consult Oracle Service 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.

TABLE 1-3 lists valid SL8500 complex ID assignments at a site.

See "Ensure the Correct Library Complex ID" on page 72 for detailed instructions.

**TABLE 1-3** 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 |

# Library Configuration Process

You use the following process to configure the libraries to send SNMP traps to STA. Perform the entire process for your library model, as per TABLE 1-4.

After you complete this process, you will configure STA to receive SNMP traps from the library (Chapter 2, Configuring SNMP in the STA Application").

**Note –** Before performing the SNMP configuration steps, see "SNMP Configuration for STA" on page 17 for important background information for these procedures.

**Note –** The SNMP configuration procedures describe the recommended v3 protocol configuration. See Appendix A, "Configuring SNMP v2c Mode" on page 197 for information on configuring the v2c protocol.

**TABLE 1-4** Steps to Configure Libraries for STA

| Step | Procedure | SL150 | SL500 | SL3000 | SL8500 |
|---|---|---|---|---|---|
| 1 | Prepare service requests for Oracle support (if not done already). See "Pre-Installation Planning" in the STA Planning and Installation Guide. | X | X | X | X |
| 2 | "Determine Configuration Parameters" on page 27 | X | X | X | X |
| 3 | "Log In to the Library" on page 30. (See "Library User Interfaces" on page 14 for important information about the available login methods.) | X | X | X | X |
| 4 | "Verify the Library Firmware Version" on page 34 | X | X | X | X |
| 5 | "Retrieve the Library IP Address" on page 36 | X | X | X | X |
| 6 | "Verify the Drive Controller Card Version" on page 41 | | | X | X |
| 7 | "Enable ADI on the Library" on page 43 (libraries with LTO drives only). | | X | X | X |
| 8 | "Enable SNMP on the Library" on page 46 | X | X | X | X |
| 9 | "Ensure an SNMP v2c User" on page 49 | X | X | X | X |
| 10 | "Create an SNMP v3 User" on page 55 | X | X | X | X |
| 11 | "Retrieve the Library SNMP Engine ID" on page 60 | | X | X | X |
| 12 | "Create an SNMP v3 Trap Recipient" on page 61 | X | X | X | X |
| 13 | "Set the SL500 Volume Label Format" on page 68 | | X | | |
| 14 | "Set the SL150 Volume Label Format" on page 70 | X | | | |
| 15 | "Set the Drive Cleaning Warning" on page 71 | | | X | X |
| 16 | "Ensure the Correct Library Complex ID" on page 72 | | | | X |

## Determine Configuration Parameters

Use TABLE 1-5 to define the configuration parameters that you will use to configure the connection between the library and the STA server.

You can use the following optional script to display the library CLI commands. It will step you through the library configuration process, request data to be entered, and then display the commands that can be copied and pasted into the library CLI.

```
/Oracle/StorageTek_Tape_Analytics/common/bin/STA-lib-config-steps.sh
```

> **Note –** Execute the script using the **sh** command. Be sure to read and understand the library configuration steps in this chapter before executing the script.

Complete the STA / Library Configuration Parameters Worksheet, TABLE 1-5 below, for your site. Then, proceed to "Log In to the Library" on page 30.

> **Note –** SNMP v3 is the recommended protocol for SNMP communications between STA and the libraries. Depending on your site requirements, however, you may choose to use v2c. TABLE 1-5 assumes you will be using the recommended v3 configuration. See Appendix A, "Configuring SNMP v2c Mode" on page 197 for information on configuring the v2c protocol.

**TABLE 1-5** STA / Library Configuration Parameters Worksheet (Sheet 1 of 3)

| Parameter | Description | Where Used | My Setting |
|---|---|---|---|
| SNMP v2c community | SNMP v2c community string.<br>**Note**: This step may be required even if you will be using SNMP v3 for STA-library communications. | Ensure an SNMP v2c User | |
| SNMP v3 user name | SNMP v3 user you create on the library. The STA server listens for traps sent by this user. Must be the same on all libraries. | Create an SNMP v3 User<br>Configure SNMP Client Settings for STA | |
| SNMP v3 user authorization password | Authorization password you assign to the SNMP v3 user. | Create an SNMP v3 User<br>Create an SNMP v3 Trap Recipient<br>Configure SNMP Client Settings for STA | |
| SNMP v3 user privacy password | Privacy password you assign to the SNMP v3 user. | Create an SNMP v3 User<br>Create an SNMP v3 Trap Recipient<br>Configure SNMP Client Settings for STA | |

**TABLE 1-5** STA / Library Configuration Parameters Worksheet (Sheet 2 of 3)

| Parameter | Description | Where Used | My Setting |
|---|---|---|---|
| SNMP traps | Traps that the library v3 user sends. Must match exactly the pre-defined list of traps the STA server listens for.<br>SL3000 and SL8500 libraries do not support trap level "4". | Create an SNMP v3 Trap Recipient | 1,2,3,4,11,21, 25,27,41,45,61, 63,65,81,85,100 |
| STA server IP address | IP address assigned to the STA server. | Create an SNMP v3 Trap Recipient<br>Configure SNMP Connections With the Library | |
| SNMP v3 recipient name | SNMP v3 trap recipient name you assign to the STA server. Must be the same on all libraries. | Create an SNMP v3 Trap Recipient | |
| Library SNMP engine ID | Globally unique SNMP engine ID assigned to the library | Create an SNMP v3 Trap Recipient<br>Configure SNMP Connections With the Library | |
| Primary library IP address | IP address of the public port on the library controller card. For SL500 libraries, this is the 1B port. For SL150 libraries, this is Network Port 1.<br>For SL3000 and SL8500 libraries, this is the 2B port. For SL3000 and SL8500 libraries using the Redundant Electronics feature, this is specifically the 2B port on the active controller card. | Configure SNMP Connections With the Library | |
| Secondary library IP address | Applies only to SL3000 and SL8500 libraries using the Dual TCP/IP or Redundant Electronics feature. See "Support for Dual TCP/IP and Redundant Electronics" on page 19 for guidelines on selecting the IP address to use. | Configure SNMP Connections With the Library | |
| Enable ADI interface | Enables the ADI drive interface on the library for LTO drives. | Enable ADI on the Library | |

**TABLE 1-5** STA / Library Configuration Parameters Worksheet (Sheet 3 of 3)

| Parameter | Description | Where Used | My Setting |
|---|---|---|---|
| Volume label formatting for SL500 libraries (two procedures) | Ensures the correct format of volume serial numbers sent to the STA server through SNMP. | Set the SL500 Volume Label Format | |
| Volume label formatting for SL150 libraries | Ensures the correct format of volume serial numbers sent to the STA server through SNMP. | Set the SL150 Volume Label Format | |
| Drive clean warning | Applies to SL3000 and SL8500 libraries only.<br>Indicates whether a drive warning should be issued whenever a library drive needs cleaning. | Set the Drive Cleaning Warning | |
| Complex ID | Applies to SL8500 libraries only.<br>Complex ID assigned to each unique library complex monitored by STA. | Ensure the Correct Library Complex ID | |

## ▼ Log In to the Library

Use this procedure to log in to the library. Before performing this procedure, you must obtain the following information from your storage administrator.

- IP address or fully qualified DNS alias of the library

  **Note –** For SL3000 and SL8500 libraries in which the Redundant Electronics feature has been installed and activated, this must be the IP address of the currently active controller.

- Password for the admin username on the library

  **Note –** See "Library User Interfaces" on page 14 for important information about the available login methods.

The log-in method depends on the library model:

- "With the CLI (all libraries except SL150)" on page 30
- "With the SL Console (all libraries except SL150)" on page 31
- "With the SL150 User Interface" on page 32

### ▼ With the CLI (all libraries except SL150)

1. **Start a terminal emulator on your PC or workstation.**
2. **Establish an SSH (secure shell) connection to the library using the IP address or DNS alias given to you by your storage administrator.**
3. **Log in to the CLI using the admin username and the password given to you by your storage administrator.**

#### *SL3000 Example*

**Note –** The SL8500 display is similar.

```
login as: admin
Using keyboard-interactive authentication.
Password: adminpwd1
***************************************************************
         SL3000 CLI Interface-Active Card-Side A

***************************************************************

SL3000>
```

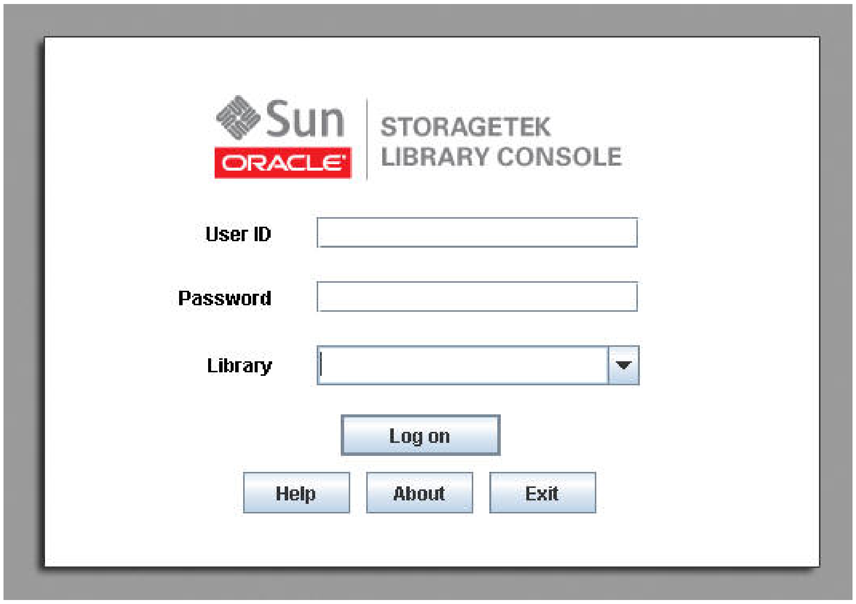
### *SL500 Example*

```
login as: admin
Using keyboard-interactive authentication.
Password: adminpwd1

Starting your CLI session ... (this may take a few seconds)

You are the only client
SL500>
```

## ▼ With the SL Console (all libraries except SL150)

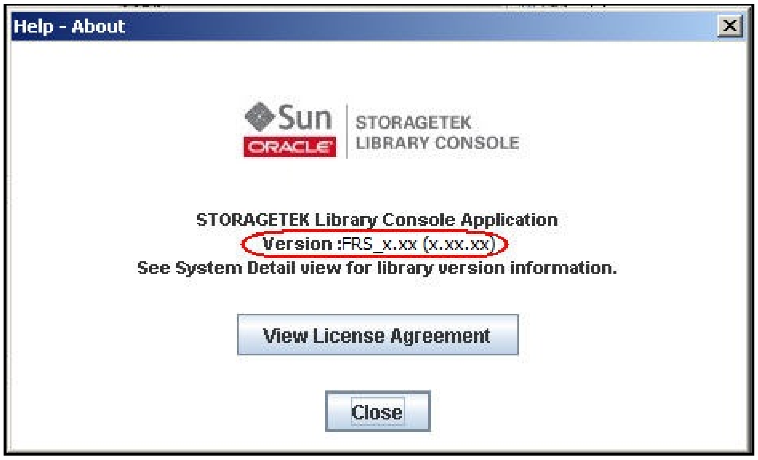
1. **Start the SL Console application on your PC or workstation.**

   The **Login** screen appears.



2. **Click the About button to display the current SL Console version and verify that it meets the STA minimum requirements.**

   **Note –** If it does not, you must install the proper version before proceeding. See the library *User's Guide* for detailed instructions.



Help - About

STORAGETEK Library Console Application
Version :FRS_x.xx (x.xx.xx)
See System Detail view for library version information.

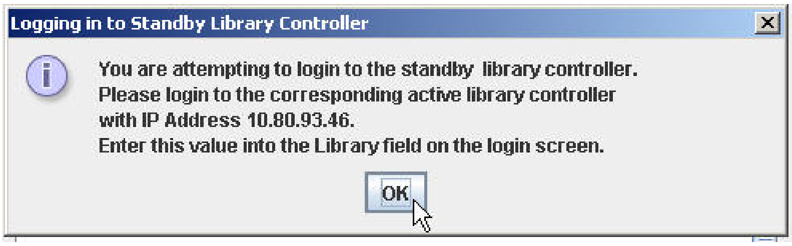
3. **Click Close to return to the Login screen.**
4. **Enter your login information.**

   **`User ID:`** admin
   **`Password:`** *password*
   **`Library:`** *library_ID*

   where:

   - User ID is **`admin`**.
   - *password* is the password assigned to this username.
   - *library_ID* is the library to which you want to connect, expressed in either of the following ways:
     - IP address of the library
     - Fully qualified DNS alias of the library
5. **Click Log on.**

   > **Note –** For SL3000 and SL8500 libraries in which the Redundant Electronics feature has been installed and activated, you can only log in to the active controller. If you attempt to log in to the standby controller, the following error is displayed. You must retry, using the correct library ID.



Logging in to Standby Library Controller

You are attempting to login to the standby library controller.
Please login to the corresponding active library controller
with IP Address 10.80.93.46.
Enter this value into the Library field on the login screen.

## ▼ With the SL150 User Interface

Log in to the SL150 browser-based user interface as follows:

1. **In a compatible browser, such as Mozilla Firefox, navigate to the hostname or IP address of the SL150 library.**

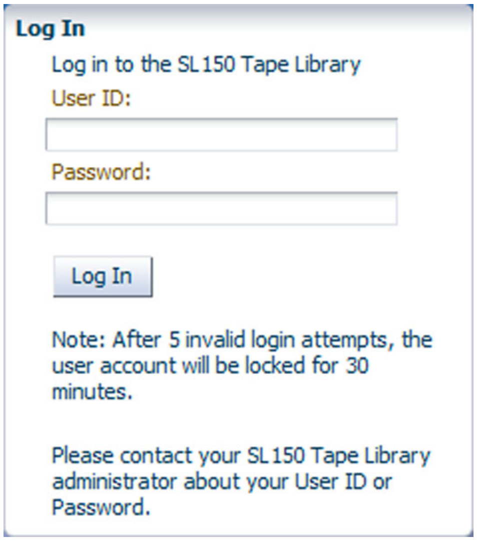
   **Note –** If this is your first time navigating to the library, you will be prompted to allow your browser to accept the connection.

2. **When the Log In dialog appears, enter your user name in the User ID text field.**

   **Note –** The User ID must have the role of administrator.

3. **Enter your password in the Password text field.**

4. **Press the Log In button.**



Log In

Log in to the SL150 Tape Library

User ID:

Password:

Note: After 5 invalid login attempts, the user account will be locked for 30 minutes.

Please contact your SL150 Tape Library administrator about your User ID or Password.

## ▼ Verify the Library Firmware Version

Use this procedure to verify that the library firmware meets or exceeds the minimum requirements for STA. For details, see the “Pre-Installation Planning” chapter within the *StorageTek Tape Analytics Planning and Installation Guide*.

For SL500 libraries, you can perform this procedure with either the CLI or the SL Console. For SL3000 and SL8500 libraries, you must use the SL Console. (Exception: If you are running FRS 8.0 on an SL8500, you can use the CLI **`version print`** command to obtain the library firmware version.) For SL150 libraries, you use the library’s browser-based user interface.

- “With the CLI (SL500 Libraries Only)” on page 34
- “With the SL Console (All libraries except SL150)” on page 34
- “With the SL150 User Interface” on page 35

### ▼ With the CLI (SL500 Libraries Only)

1. **Display version information for the library.**

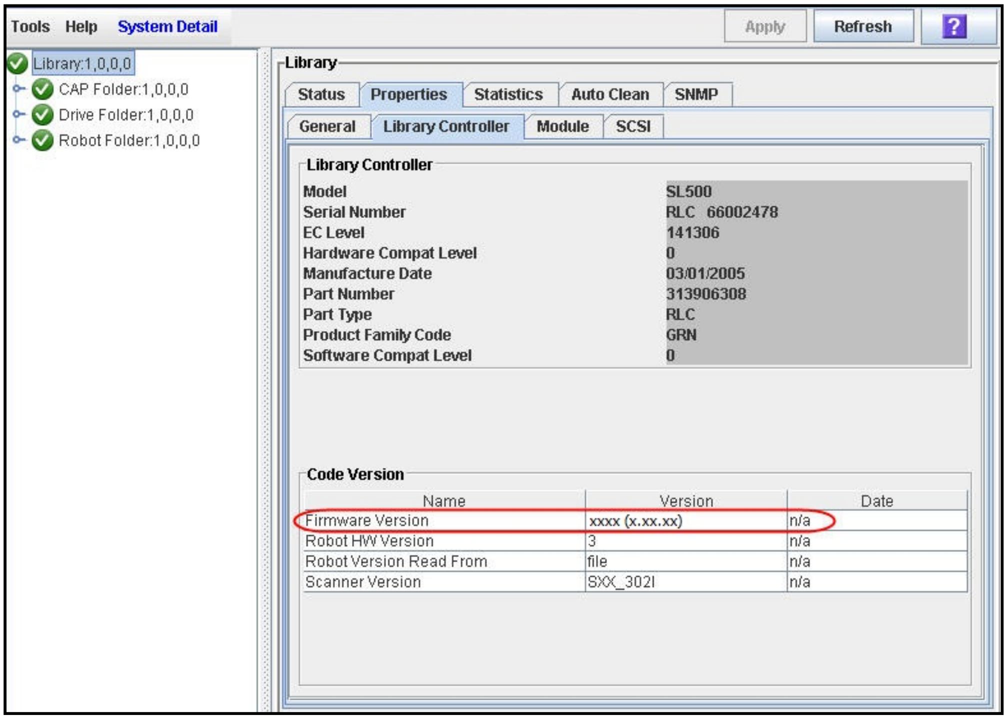
```
SL500> version print
Library Hardware Information
  Library Vendor:       STK
  Library Model:        SL500
  Serial Number:        759010203285
  Host Interface:       Fibre
Library Active Software Information
  Firmware Version:     xxxx (x.xx.xx)

OK
SL500>
```

> **Note –** If the screen displays **`SYNTAX ERROR!!`**, the library firmware is down-level. Contact your Oracle support representative to upgrade the firmware.

2. **Determine whether the displayed version meets the minimum requirements for STA.**
   - If it does, then proceed to “Retrieve the Library IP Address” on page 36.
   - If it does not, then contact your Oracle support representative to upgrade the firmware.

### ▼ With the SL Console (All libraries except SL150)

1. **Log in to the library with the SL Console.**
2. **Select System Detail > Library > Properties > Library Controller.**



Library Controller

| | |
|---|---|
| Model | SL500 |
| Serial Number | RLC 66002478 |
| EC Level | 141306 |
| Hardware Compat Level | 0 |
| Manufacture Date | 03/01/2005 |
| Part Number | 313906308 |
| Part Type | RLC |
| Product Family Code | GRN |
| Software Compat Level | 0 |

Code Version

| Name | Version | Date |
|---|---|---|
| Firmware Version | xxxx (x.xx.xx) | n/a |
| Robot HW Version | 3 | n/a |
| Robot Version Read From | file | n/a |
| Scanner Version | SXX_302I | n/a |

3. **Determine whether the displayed version meets the minimum requirements for STA.**

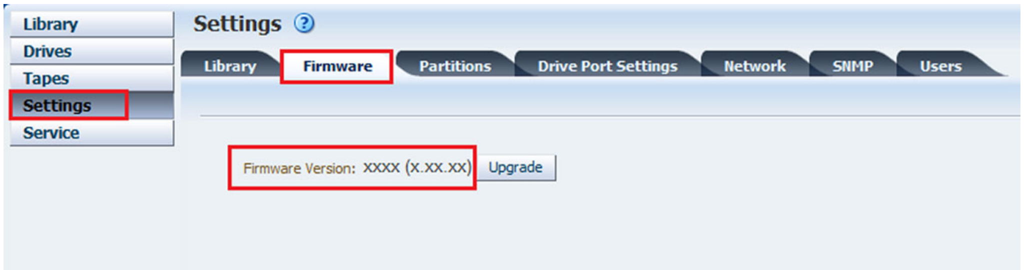
   - If it does, then proceed to either "Retrieve the Library IP Address" on page 36 or "Retrieve SL3000 or SL8500 IP Addresses" on page 36, depending on the library model.
   - If it does not, then contact your Oracle support representative to upgrade the firmware.

## ▼ With the SL150 User Interface

1. **Log in to the library's browser-based user interface.**
2. **Select Settings from the navigation bar on the left side of the interface.**
3. **Select the Firmware tab.**

   The firmware version is displayed.

   > **Note –** Alternately, you can click the About button in the lower-right corner of the screen to obtain the firmware version.



Firmware Version: XXXX (X.XX.XX)

# ▼ Retrieve the Library IP Address

Use this procedure to retrieve and record the library IP address, which you will use later when you configure the STA connection with the library (see "Configure SNMP Connections With the Library" on page 84).

The procedure you follow depends on the library model:

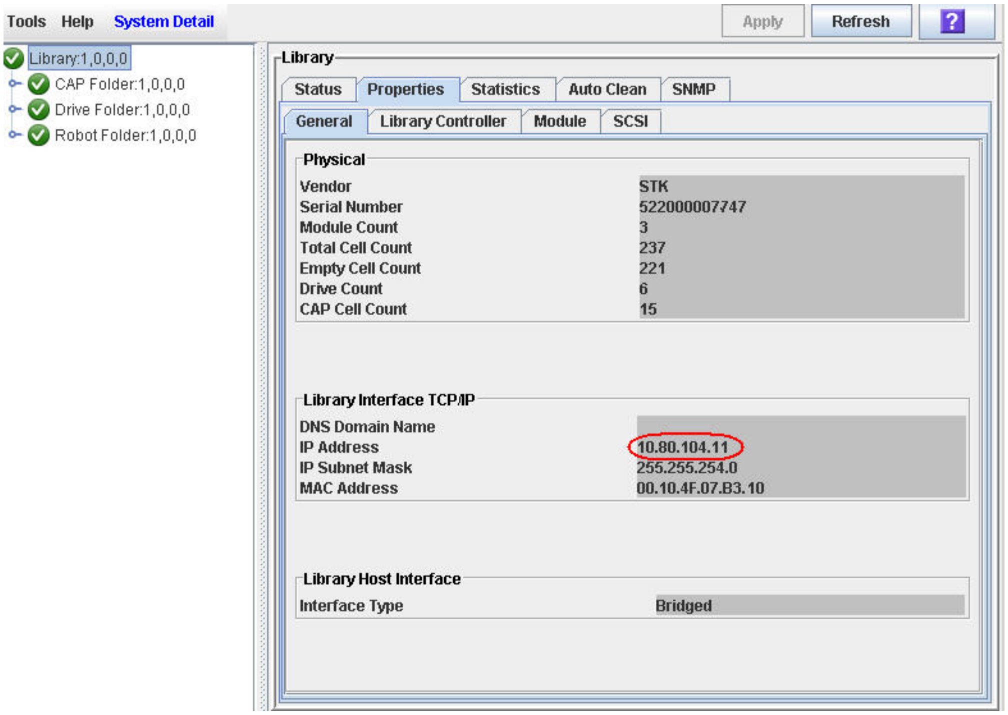
- "Retrieve the SL500 IP Address" on page 36
- "Retrieve SL3000 or SL8500 IP Addresses" on page 36
- "Retrieve the SL150 IP Address" on page 40

## ▼ Retrieve the SL500 IP Address

**Note –** You must perform this procedure from the SL Console.

1. **Log in to the library with the SL Console.**
2. **Select System Detail > Library > Properties > General.**

   The library IP address is listed in the "Library Interface TCP/IP" section.



Physical

| | |
|---|---|
| Vendor | STK |
| Serial Number | 522000007747 |
| Module Count | 3 |
| Total Cell Count | 237 |
| Empty Cell Count | 221 |
| Drive Count | 6 |
| CAP Cell Count | 15 |

Library Interface TCP/IP

| | |
|---|---|
| DNS Domain Name | |
| IP Address | 10.80.104.11 |
| IP Subnet Mask | 255.255.254.0 |
| MAC Address | 00.10.4F.07.B3.10 |

Library Host Interface

| | |
|---|---|
| Interface Type | Bridged |

3. **Record the library IP address as the primary library IP address.**
4. **Proceed to "Enable ADI on the Library" on page 43.**

## ▼ Retrieve SL3000 or SL8500 IP Addresses

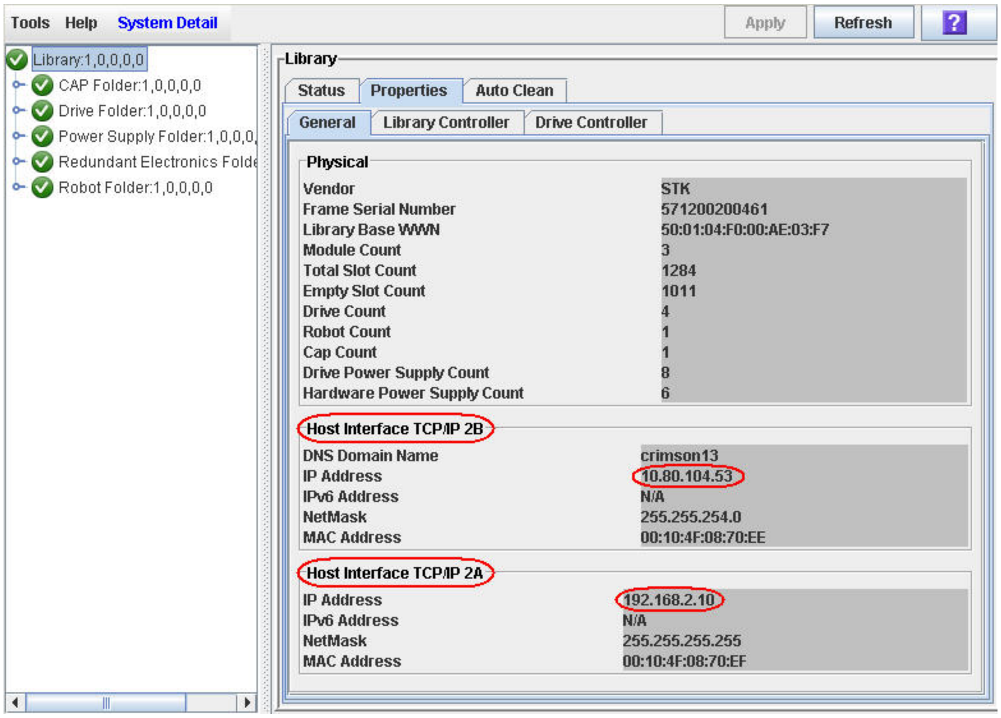
Before performing this procedure, you must determine whether you want to configure STA to support either Dual TCP/IP or Redundant Electronics, which are optional features for the library. See "Support for Dual TCP/IP and Redundant Electronics" on page 19 for details.

**Note –** You must perform this procedure from the SL Console.

1. **Log in to the library with the SL Console.**
2. **Proceed as follows, based on how you want to configure STA:**
   - If you want to configure STA to support the optional Dual TCP/IP feature, go to Step 3.
   - If you want to configure STA to support the optional Redundant Electronics feature, go to Step 4.
   - If the library does not include either of these features, go to Step 5.
3. **To retrieve library IP addresses for Dual TCP/IP support:**

   a. **Select System Detail > Library > Properties > General.**

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



Physical

| | |
|---|---|
| Vendor | STK |
| Frame Serial Number | 571200200461 |
| Library Base WWN | 50:01:04:F0:00:AE:03:F7 |
| Module Count | 3 |
| Total Slot Count | 1284 |
| Empty Slot Count | 1011 |
| Drive Count | 4 |
| Robot Count | 1 |
| Cap Count | 1 |
| Drive Power Supply Count | 8 |
| Hardware Power Supply Count | 6 |

Host Interface TCP/IP 2B

| | |
|---|---|
| DNS Domain Name | crimson13 |
| IP Address | 10.80.104.53 |
| IPv6 Address | N/A |
| NetMask | 255.255.254.0 |
| MAC Address | 00:10:4F:08:70:EE |

Host Interface TCP/IP 2A

| | |
|---|---|
| IP Address | 192.168.2.10 |
| IPv6 Address | N/A |
| NetMask | 255.255.255.255 |
| MAC Address | 00:10:4F:08:70:EF |

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

   b. **Record the library IP address(es) as follows:**

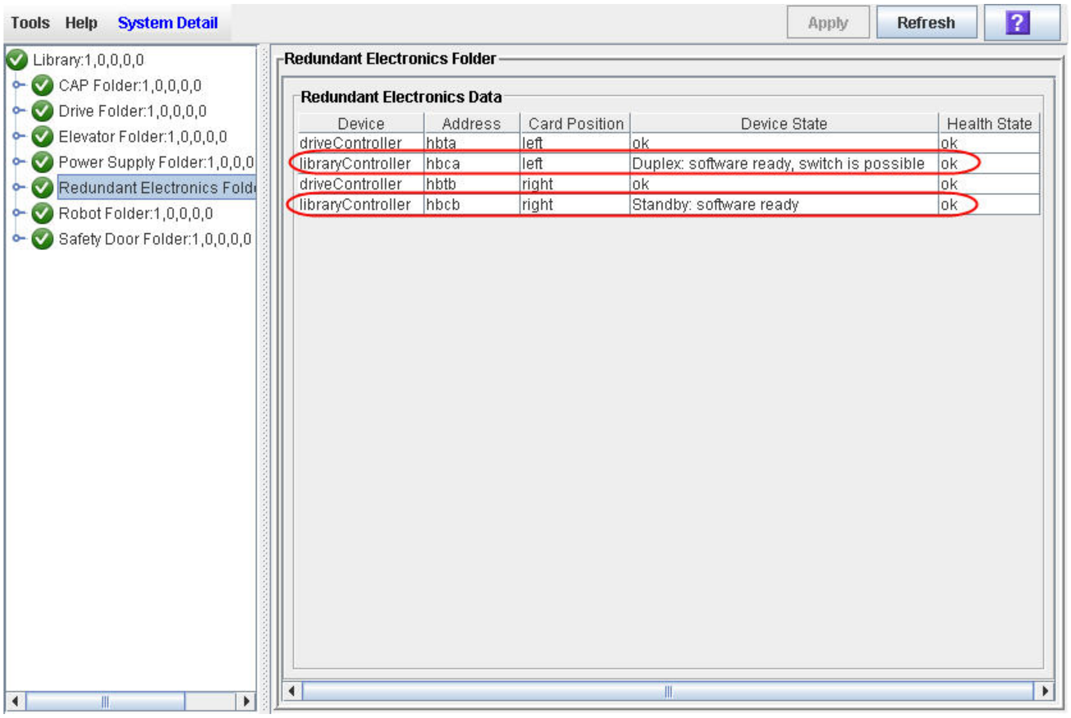
   - The Primary library IP address is displayed in the 2B section.
   - The secondary library IP address is displayed in the 2A section.

   c. **Proceed to Step 6.**

4. **To retrieve library IP addresses for Redundant Electronics support:**

   a. **Select Tools > System Detail, and select the Redundant Electronics folder.**

**Note –** If this folder is not listed, the Redundant Electronics feature is not available on the library.



Tools
Help
System Detail
Apply
Refresh
?
Library:1,0,0,0,0
CAP Folder:1,0,0,0,0
Drive Folder:1,0,0,0,0
Elevator Folder:1,0,0,0,0
Power Supply Folder:1,0,0,0
Redundant Electronics Fold
Robot Folder:1,0,0,0,0
Safety Door Folder:1,0,0,0,0
Redundant Electronics Folder

Redundant Electronics Data

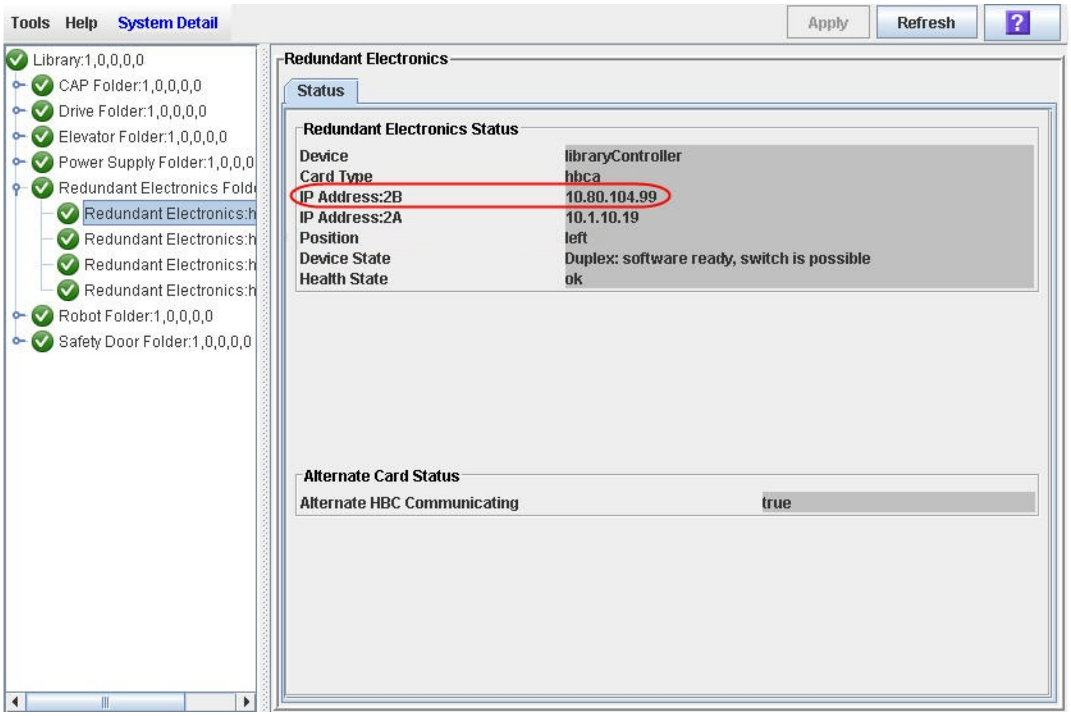
| Device | Address | Card Position | Device State | Health State |
|---|---|---|---|---|
| driveController | hbta | left | ok | ok |
| libraryController | hbca | left | Duplex: software ready, switch is possible | ok |
| driveController | hbtb | right | ok | ok |
| libraryController | hbcb | right | Standby: software ready | ok |

b. **Verify the following entries in the Device State field:**

- One library controller card indicates “Duplex: software ready, switch is possible”. This is the current active controller and could be either the hbca or hbcb card.
- The other library controller card indicates “Standby: software ready”. This is the current alternate controller.

These entries indicate that the controller cards are functioning normally. If either entry does not match, then contact your Oracle support representative before proceeding.

c. **Expand the Redundant Electronics folder, and select the active controller card.**



Redundant Electronics Status

| | |
|---|---|
| Device | libraryController |
| Card Type | hbca |
| IP Address:2B | 10.80.104.99 |
| IP Address:2A | 10.1.10.19 |
| Position | left |
| Device State | Duplex: software ready, switch is possible |
| Health State | ok |

Alternate Card Status

| | |
|---|---|
| Alternate HBC Communicating | true |

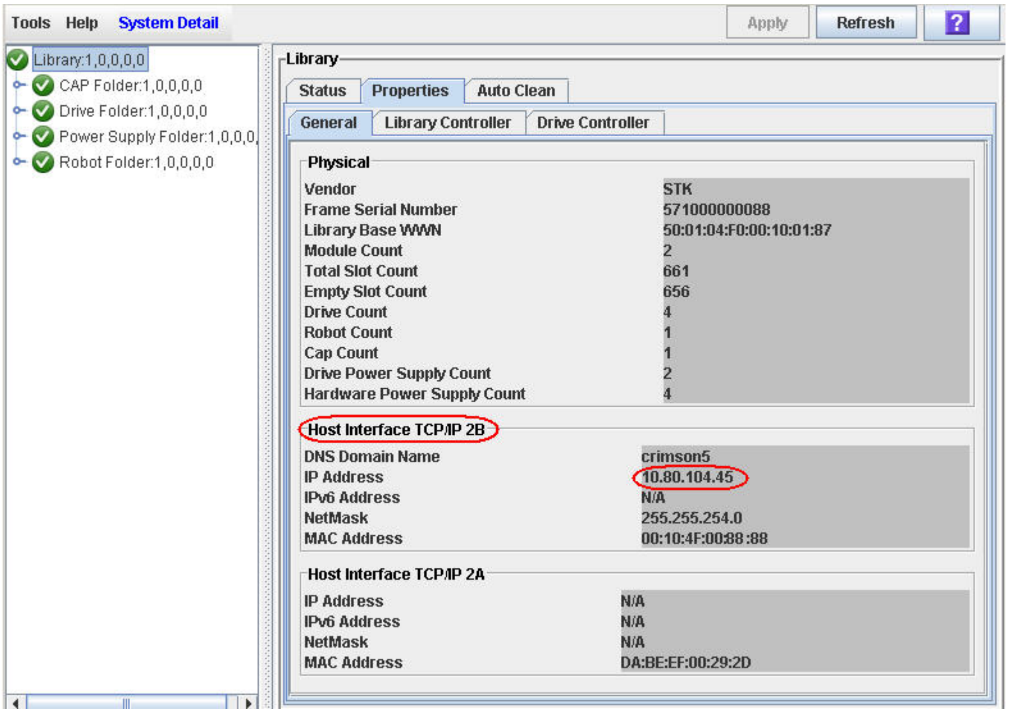
d. **Record the IP address of the 2B port.**

e. **Repeat Step c and Step d for the alternate (standby) controller card.**

5. **To retrieve the IP address for libraries with neither Dual TCP/IP nor Redundant Electronics:**

   a. **Select Tools > System Detail > Library > Properties > General.**

      The IP address information is displayed in the Host Interface TCP/IP 2B section. There is no IP address information in the 2A section.



Physical

| | |
|---|---|
| Vendor | STK |
| Frame Serial Number | 571000000088 |
| Library Base WWN | 50:01:04:F0:00:10:01:87 |
| Module Count | 2 |
| Total Slot Count | 661 |
| Empty Slot Count | 656 |
| Drive Count | 4 |
| Robot Count | 1 |
| Cap Count | 1 |
| Drive Power Supply Count | 2 |
| Hardware Power Supply Count | 4 |

Host Interface TCP/IP 2B

| | |
|---|---|
| DNS Domain Name | crimson5 |
| IP Address | 10.80.104.45 |
| IPv6 Address | N/A |
| NetMask | 255.255.254.0 |
| MAC Address | 00:10:4F:00:88:88 |

Host Interface TCP/IP 2A

| | |
|---|---|
| IP Address | N/A |
| IPv6 Address | N/A |
| NetMask | N/A |
| MAC Address | DA:BE:EF:00:29:2D |

b. Record the IP address as the primary library IP address.

6. Proceed to "Verify the Drive Controller Card Version" on page 41.

## ▼ Retrieve the SL150 IP Address

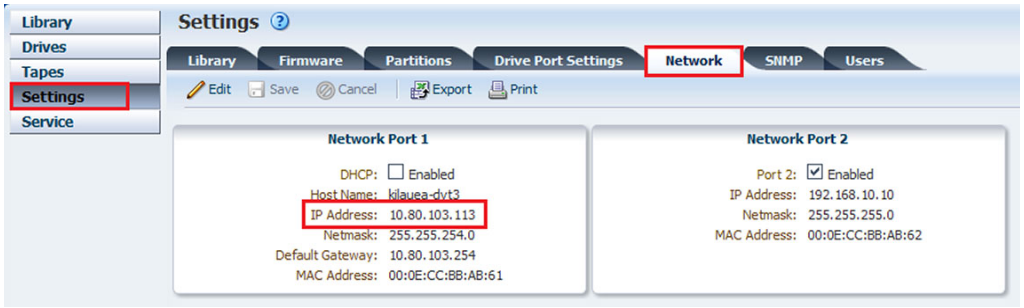
1. Log in to the library's browser-based user interface.

2. Select Settings from the navigation bar on the left side of the interface.

3. Select the Network tab.

   The library IP address is displayed under the **Network Port 1** section. (The **Network Port 2** section is reserved for service use.)

   > **Note –** DHCP should not be enabled. A statically-assigned IP address is recommended for communications with STA.



Network Port 1

DHCP: □ Enabled
Host Name: kilauea-dvt3
IP Address: 10.80.103.113
Netmask: 255.255.254.0
Default Gateway: 10.80.103.254
MAC Address: 00:0E:CC:BB:AB:61

Network Port 2

Port 2: ☑ Enabled
IP Address: 192.168.10.10
Netmask: 255.255.255.0
MAC Address: 00:0E:CC:BB:AB:62

## ▼ Verify the Drive Controller Card Version

**Note –** This procedure applies only to SL3000 and SL8500 libraries.

Use the SL Console to verify that a high-memory drive controller (HBT) card is installed in the library and that the card has the correct code version. Without a high-memory HBT card, the library will not supply richer drive data to STA from StorageTek and LTO drives. In addition, you will not be able to enable the ADI interface on the library if you have LTO drives. See "Drive ADI Interface" on page 21 for additional information.

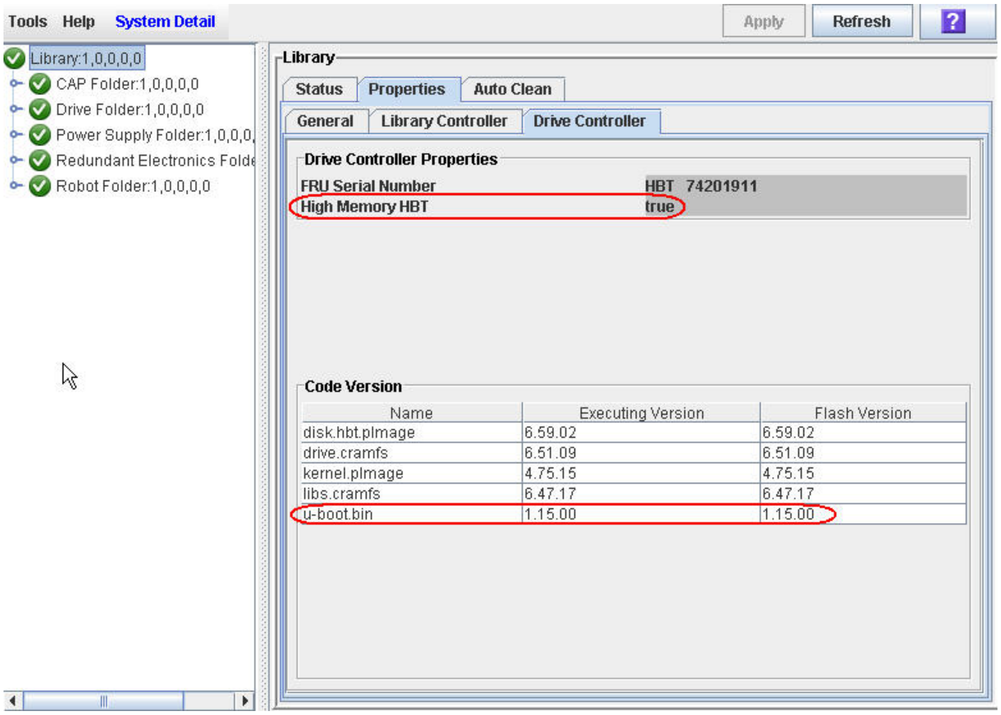
**Note –** All SL3000 libraries are shipped with the high-memory card, as are all SL8500 libraries beginning from 2006. Nevertheless, it is recommended that you use this procedure to verify the correct configuration.

**Note –** SL8500 FRS 8.0 allows the CLI `config print` command to be used to obtain HBT card information, in addition to the SL Console.

**Note –** If you have an SL8500 or SL3000 with Redundant Electronics, the following procedure checks the memory status of the active HBT card only. However, if you are running FRS 8.0 on an SL8500, you can check the memory status of both the active and standby HBT cards within the Redundant Electronics folder in the device tree. To do so, expand the Redundant Electronics folder, then select each HBT card (hbta, hbtb).

1. **Select Tools > System Detail > Library > Properties > Drive Controller.**

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



Drive Controller Properties

FRU Serial Number HBT 74201911

High Memory HBT true

Code Version

| Name | Executing Version | Flash Version |
|---|---|---|
| disk.hbt.plmage | 6.59.02 | 6.59.02 |
| drive.cramfs | 6.51.09 | 6.51.09 |
| kernel.plmage | 4.75.15 | 4.75.15 |
| libs.cramfs | 6.47.17 | 6.47.17 |
| u-boot.bin | 1.15.00 | 1.15.00 |

2. **Verify the following information on the screen:**

    - High Memory HBT indicates “true”.
    - “u-boot.bin” is listed in the Code Version table.

    If High Memory HBT indicates “low” or the “u-boot.bin” entry is missing, then contact your Oracle support representative.

# ▼ Enable ADI on the Library

**Note –** This procedure does not apply to the SL150 library.

**Note –** This procedure applies only if the library already includes or will include HP or IBM LTO drives (LTO-3, LTO-4, LTO-5, or LTO-6[1]) in the near future. For SL500 libraries, this procedure is required because LTO is the only drive type that provides rich data to STA from the SL500.

**Note –** For SL3000 and SL8500 libraries, before performing this procedure, you must verify that a high-memory drive controller (HBT) card is installed in the library. See "Verify the Drive Controller Card Version" on page 41 for details.

**Note –** If you have an SL3000 or SL8500 licensed for Redundant Electronics, both the active and standby HBT cards must have high memory. If you have an SL8500 running FRS 8.0, the **`drive adiEnable on`** command will fail if Redundant Electronics is licensed and either 1) the active HBT card is low-memory, 2) the standby HBT card is low-memory, or 3) the standby HBT card is not communicating or not installed.

**Note –** Your Oracle support representative may have already enabled ADI on your library if you have IBM LTO drives and you submitted a service request to manually enable ADI on those drives.

Use this procedure to ensure that the ADI drive interface is enabled on the library. The ADI interface must be enabled on both the library and the LTO drives for the library to be able to send rich LTO data to STA. See "Drive ADI Interface" on page 21 for additional information.

If you change the ADI interface setting, you must reboot the library for the change to take effect.

**Note –** You must use the CLI for this procedure. However, the syntax of the commands varies by library model. See "For SL3000 or SL8500 Libraries" or "For SL500 Libraries", below.

## ▼ For SL3000 or SL8500 Libraries

1. **Use the following command to display the current status of the ADI interface:**

   ```
   drive adiEnable print
   ```

   - If Adi Status is "true", as in the following example, then ADI is already enabled on the library, and you can proceed to "Create an SNMP v3 User" on page 55.

[1] At the time of STA 1.0.2 release, HP LTO-6 drives are not supported.

```
SL3000> drive adiEnable print
   requestId
   requestId 12345
   Attributes Adi Status true
   Object     Library    1,0,0,0,0

   Done

COMPLETED
```

- If Adi Status is "false", as in the following example, then go to Step 2, below.

```
SL3000> drive adiEnable print
   requestId
   requestId 12345
   Attributes Adi Status false
   Object     Library    1,0,0,0,0

   Done

COMPLETED
```

2. **Enable the ADI interface on the library.**

```
SL3000> drive adiEnable on
   requestID
   requestID 12345
   Success true
   Done
COMPLETED
```

3. **Reboot the library to activate the change. See the "SL Console Diagnostics and Utilities" chapter of your library** *User's Guide* **for instructions.**

4. **Proceed to "Enable SNMP on the Library" on page 46.**

## ▼ For SL500 Libraries

1. **Use the following command to display the current status of the ADI interface:**

   `enableADI print`

   - If Adi Status is "on", as in the following example, then ADI is already enabled on the library, and you can proceed to "Enable SNMP on the Library" on page 46.

```
SL500> enableADI print
enableADI set to: on
OK
```

- If Adi Status is "off", as in the following example, then go to Step 2, below.

```
SL500> enableADI print
enableADI set to: off
OK
```

2. **Enable the ADI interface on the library.**

```
SL500> enableADI on
NOTE - Changing of ADI enable will take effect only
       after the drive or library is rebooted.

  enableADI set to: on
OK
```

3. **Reboot the library to activate the change. See the "SL Console Diagnostics and Utilities" chapter of your library** *User's Guide* **for instructions.**

4. **Proceed to "Enable SNMP on the Library" on page 46.**

# ▼ Enable SNMP on the Library

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

> **Note –** For SL500 libraries, you can choose to perform this procedure with either the CLI or the SL Console. For SL3000 and SL8500 libraries, you must use the CLI. For SL150 libraries, you use the library's browser-based user interface.

## ▼ With the CLI

1. **Ensure that SNMP is enabled on the public port.**

   - For SL3000 and SL8500 libraries, you must enable SNMP on Port 2B.

     > **Note –** If the library includes the Dual TCP/IP feature, this command enables SNMP on both the 2B and the 2A port; you do not need to issue a separate command for the 2A port.

```
SL3000> snmp enable port2b
   requestId
   requestId 12345
   Device 1,0,0,0,1
   Success true
   Done
   Failure Count 0
   Success Count 1
COMPLETED
```

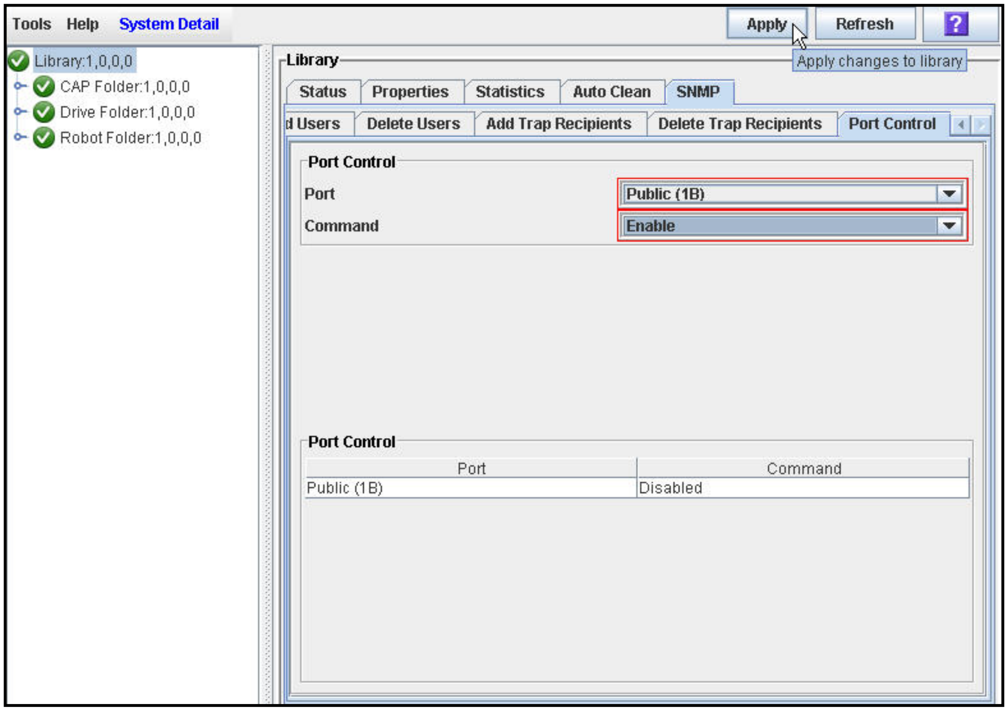
   - For SL500 libraries, you must enable SNMP on Port 1B.

```
SL500> snmp enable port1B
   requestId
   requestId 12345
   Device 1,0,0,0
   Success true
   Done
   Failure Count 0
   Success Count 1
COMPLETED
```

2. **Proceed to "Ensure an SNMP v2c User" on page 49.**

## ▼ With the SL Console (SL500 only)

1. **Select System Detail > Library > SNMP >Port Control.**
2. **Complete the Port Control tab as follows:**
   - **Port** – Select Public 1B in the menu.
   - **Command** – Select Enable in the menu.



Port Control

Port: Public (1B)

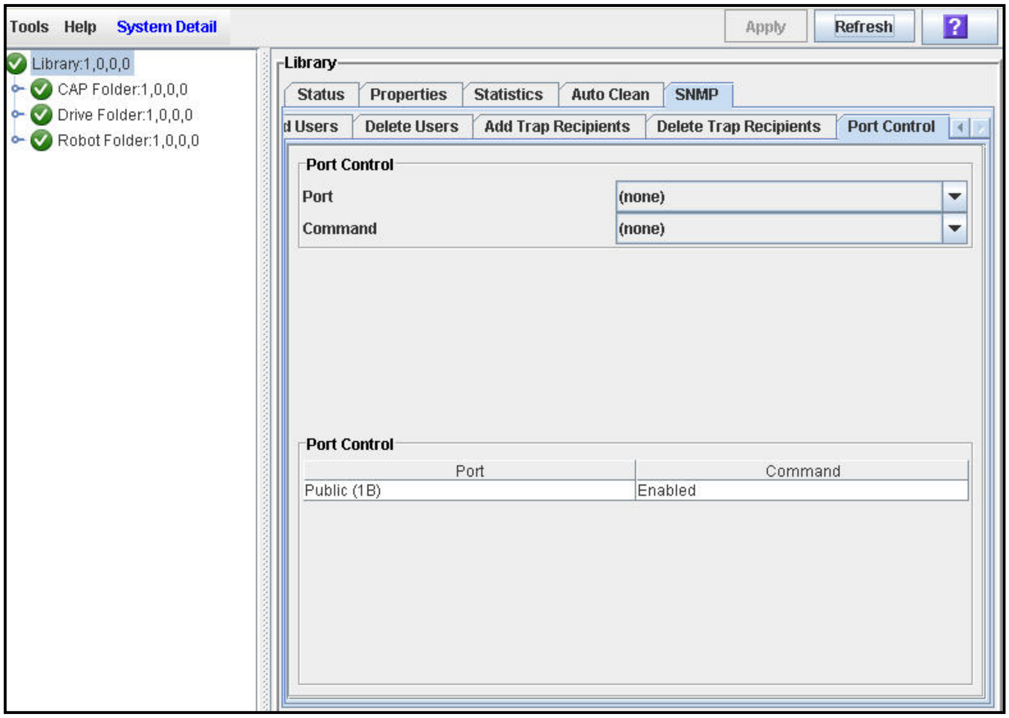
Command: Enable

Port Control

| Port | Command |
|---|---|
| Public (1B) | Disabled |

3. **Click Apply.**

   SNMP is enabled on the port, and the status is updated.



Port Control

Port: (none)

Command: (none)

Port Control

| Port | Command |
|---|---|
| Public (1B) | Enabled |

4. **Proceed to "Ensure an SNMP v2c User" on page 49.**

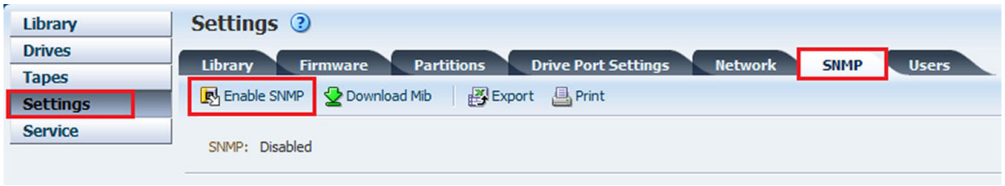
## ▼ With the SL150 User Interface

By default, the SL150 library ships with SNMP disabled. To enable SNMP, perform the following.

1. **Select Settings from the navigation bar on the left side of the interface.**

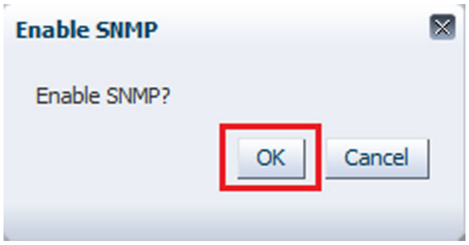
2. **Select the SNMP tab.**

3. **Select Enable SNMP.**



SNMP: Disabled

4. **In the confirmation window, click OK.**



Enable SNMP?

5. **Proceed to "Ensure an SNMP v2c User" on page 49.**

## ▼ Ensure an SNMP v2c User

A v2c user is required only if one of the following conditions is true:

- You intend to use v2c for STA communication

  See Appendix A, "Configuring SNMP v2c Mode" on page 197 for information on configuring the v2c protocol. SNMP v3 is the recommended protocol for STA communication. For more information, see "SNMP Configuration for STA" on page 17.

- You have an SL500 library with firmware below version FRS 1482

- You have an SL3000 library with firmware below version FRS 4.0

  If your firmware is below one of the above versions, the initial handshake between the library and the STA server is established through the v2c user.

> **Note –** See the "Library Software Requirements" section within the *STA Planning and Installation Guide* for the minimum library firmware required by STA.
>
> **Note –** There must be one and only one v2c user on the library. If one already exists, you should not create a second one.
>
> **Note –** You should not remove an existing v2c "public" user without consulting Oracle Service. In some cases, a v2c "public" user is required for communications between the library and Oracle Service Delivery Platform (SDP).

For SL500 libraries, you can choose to perform this procedure with either the CLI or the SL Console. For SL3000 and SL8500 libraries, you must use the CLI. For SL150 libraries, you use the browser-based user interface.

### ▼ With the CLI (All libraries except SL150)

1. **Use the following command to determine whether a v2c user already exists:**

   ```
   snmp listUsers
   ```

   - If a v2c user is already defined, as in the following example, proceed to "Create an SNMP v3 User" on page 55.

     > **Note –** An existing v2c user is commonly set to the "public" community, but depending on your existing configuration, may be defined in another community name.

```
SL500> snmp listUsers
   requestId
   requestId 12345
   Attributes Community public
              Index     1
              Version   v2c
   Object     Snmp      snmp
   Done
   Failure Count 0
   Success Count 1
COMPLETED
OK
```

- If there is no v2c user, as in the following example, go to Step 2, below.

```
SL500> snmp listUsers
   requestId
   requestId 12345
   Done
   Failure Count 0
   Success Count 1
COMPLETED
OK
```

2. **Use the following command to add the SNMP v2c user:**

   **`snmp addUser version`** *version* **`community`** *community_name*

   Where:

   - *version* is always **`v2c`**
   - *community_name* can be **`public`**, or another name of your choice.

```
SL3000> snmp addUser version v2c community public
   requestId
   requestId 12345
   Device 1,0,0,0
   Success true
   Done
   Failure Count 0
   Success Count 1
COMPLETED
OK
```

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

```
SL3000> snmp listUsers
   requestId
   requestId 12345
   Attributes Community public
              Index     1
              Version   v2c
   Object     Snmp      snmp
   Done
   Failure Count 0
   Success Count 1
COMPLETED
OK
```

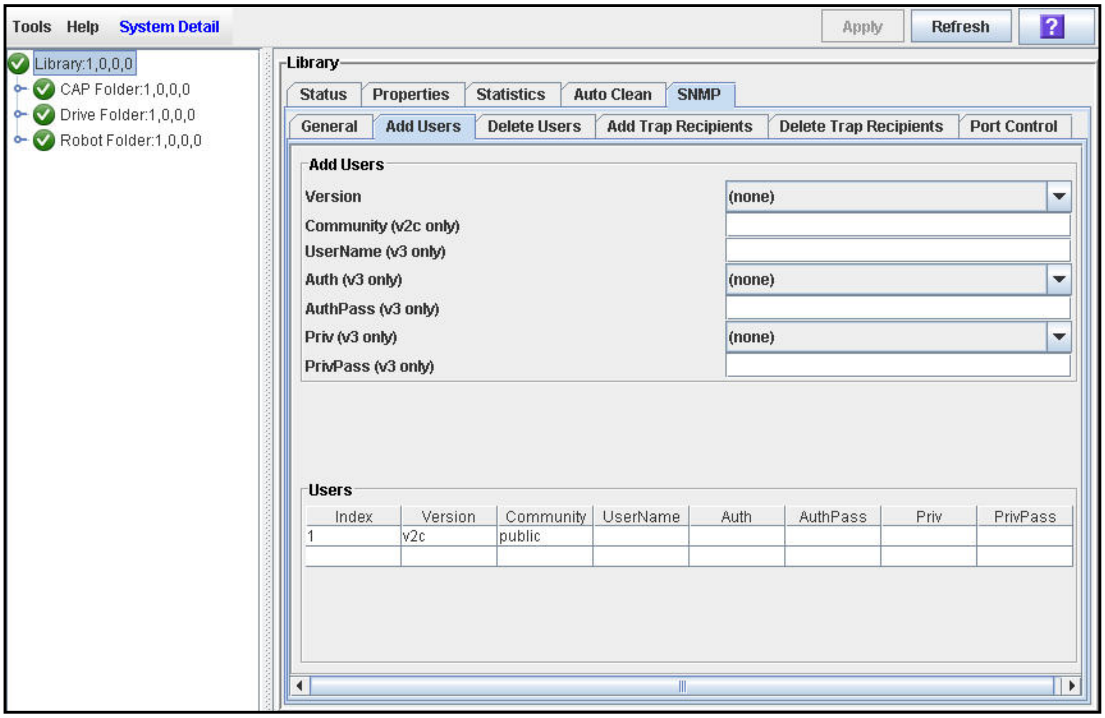
4. **Proceed to "Create an SNMP v3 User" on page 55.**

## ▼ With the SL Console (SL500 only)

1. **To determine whether a v2c user already exists, select System Detail > Library > SNMP > Add Users.**

   - If a v2c user is already defined, as in the following example, proceed to "Create an SNMP v3 User" on page 55.

     **Note –** An existing v2c user is commonly set to the "public" community, but depending on your existing configuration, may be defined in another community name.



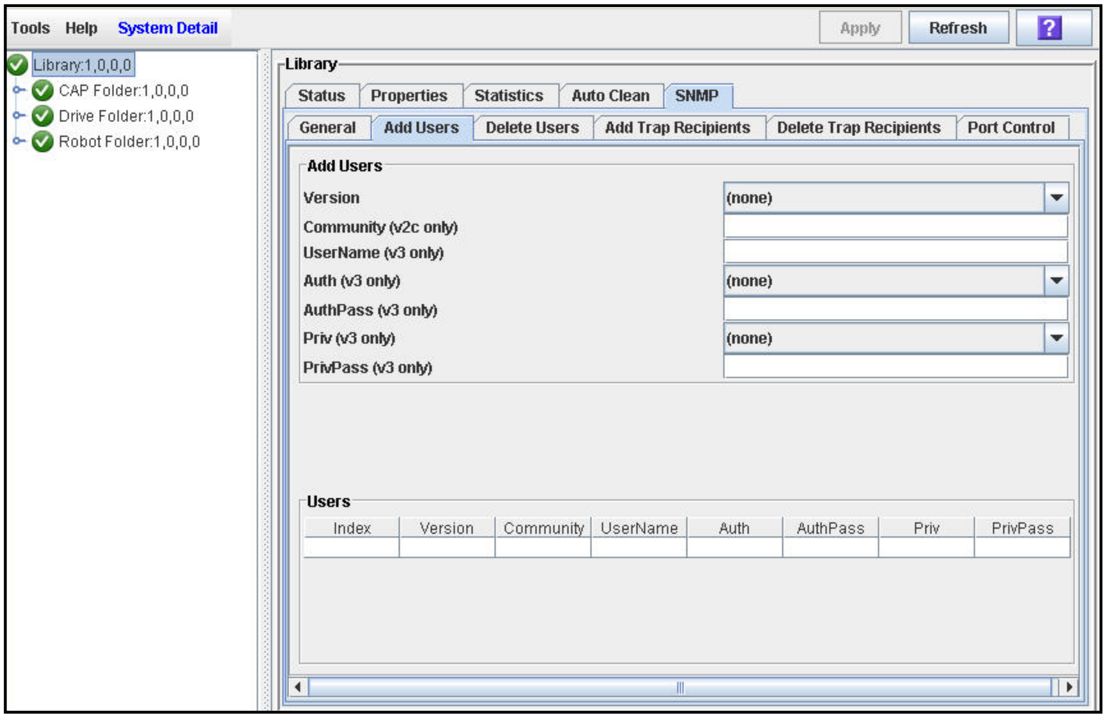
Add Users

| | |
|---|---|
| Version | (none) |
| Community (v2c only) | |
| UserName (v3 only) | |
| Auth (v3 only) | (none) |
| AuthPass (v3 only) | |
| Priv (v3 only) | (none) |
| PrivPass (v3 only) | |

Users

| Index | Version | Community | UserName | Auth | AuthPass | Priv | PrivPass |
|---|---|---|---|---|---|---|---|
| 1 | v2c | public | | | | | |

   - If there is no v2c user, as in the following example, proceed to Step 2 of this procedure.



Add Users

Version (none)

Community (v2c only)

UserName (v3 only)

Auth (v3 only) (none)

AuthPass (v3 only)

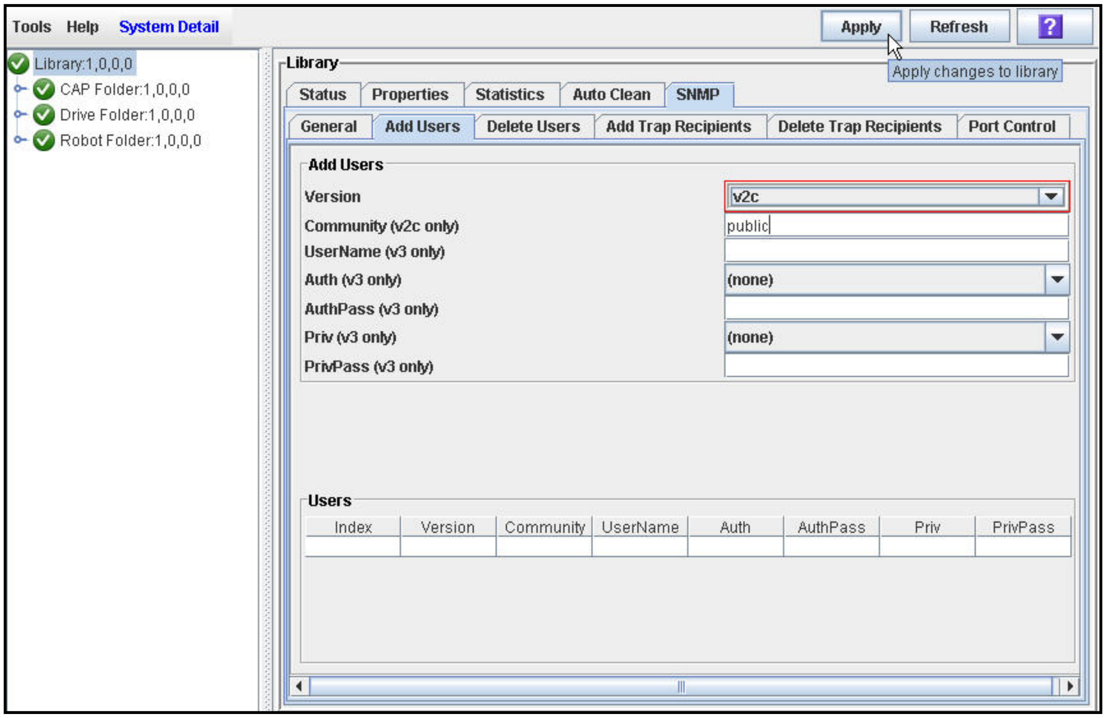
Priv (v3 only) (none)

PrivPass (v3 only)

Users

| Index | Version | Community | UserName | Auth | AuthPass | Priv | PrivPass |
|---|---|---|---|---|---|---|---|

2. **To add the SNMP v2c user, complete the Add Users tab as follows:**
   - **Version** – Select v2c from the menu.
   - **Community** – Can be **`public`**, or another name of your choice.



Add Users

Version v2c

Community (v2c only) public

UserName (v3 only)

Auth (v3 only) (none)

AuthPass (v3 only)

Priv (v3 only) (none)

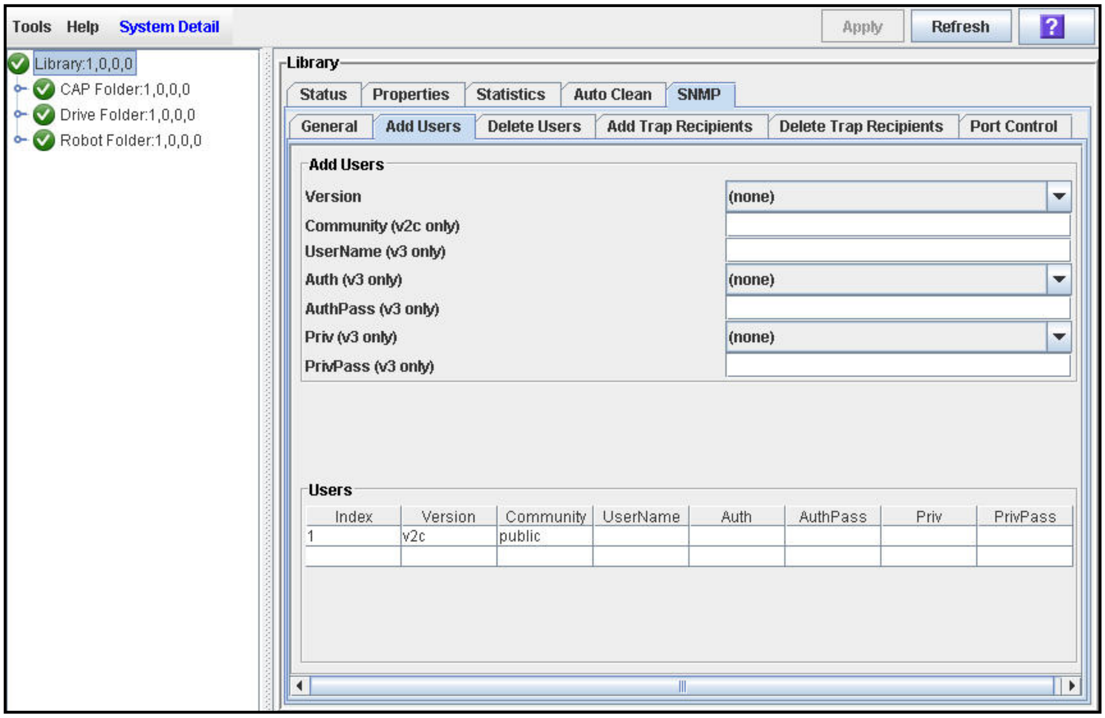
PrivPass (v3 only)

Users

| Index | Version | Community | UserName | Auth | AuthPass | Priv | PrivPass |
|---|---|---|---|---|---|---|---|

3. **Click Apply.**

The user is added and the screen is updated.



Add Users

| | |
|---|---|
| Version | (none) |
| Community (v2c only) | |
| UserName (v3 only) | |
| Auth (v3 only) | (none) |
| AuthPass (v3 only) | |
| Priv (v3 only) | (none) |
| PrivPass (v3 only) | |

Users

| Index | Version | Community | UserName | Auth | AuthPass | Priv | PrivPass |
|---|---|---|---|---|---|---|---|
| 1 | v2c | public | | | | | |

4. **Proceed to “Create an SNMP v3 User” on page 55.**

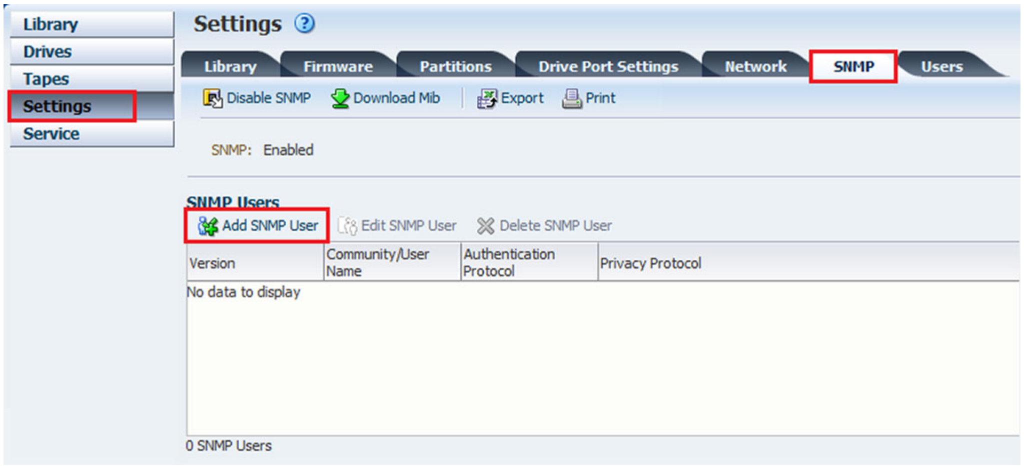
## ▼ With the SL150 User Interface

By default, the SL150 ships without a v2c user defined. If you plan to use v2c for STA communications, create a v2c user as follows.

1. **Select Settings from the navigation bar on the left side of the interface.**

2. **Select the SNMP tab.**

3. **Under the SNMP Users section, select Add SNMP User.**



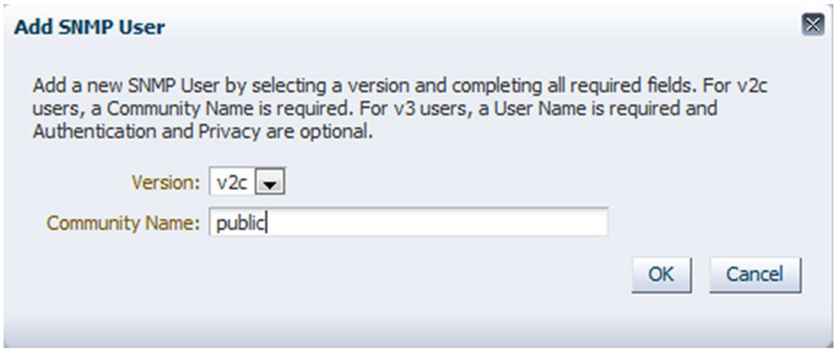
SNMP: Enabled

SNMP Users

| Version | Community/User Name | Authentication Protocol | Privacy Protocol |
|---|---|---|---|
| No data to display | | | |

0 SNMP Users

4. **In the Add SNMP User screen, complete the information as follows:**
   - **Version –** Select v2c
   - **Community Name –** Can be **`public`**, or another name of your choice.
5. **Click OK.**



Add SNMP User

Add a new SNMP User by selecting a version and completing all required fields. For v2c users, a Community Name is required. For v3 users, a User Name is required and Authentication and Privacy are optional.

Version: v2c

Community Name: public

# ▼ Create an SNMP v3 User

Use this procedure to create an SNMP v3 user for the library. All SNMP traps and MIB (management information base) data are sent to the STA server through the v3 user.

You must specify authorization and privacy mechanisms and passwords for the v3 user. For STA, the authorization method is always SHA (Secure Hash Algorithm), and the privacy method is always DES (Data Encryption Standard).

> **Caution –** Take care when entering the usernames and passwords in this procedure, and keep track of your entries. Later, you must enter the same information on the STA server, and if your entries do not match, the STA SNMP connection with the library will fail. See "Configure SNMP Client Settings for STA" on page 80.

> **Note –** Before performing this procedure, you may need to create a v2c user. See "Ensure an SNMP v2c User" on page 49 for details.

> **Note –** The SNMP v3 trap user you create in this procedure must have the same name as the SNMP v3 recipient you create next. See "Create an SNMP v3 Trap Recipient" on page 61.

For SL500 libraries, you can choose to perform this procedure with either the CLI or the SL Console. For SL3000 and SL8500 libraries, you must use the CLI. For SL150 libraries, you use the browser-based user interface.

## ▼ With the CLI (All Libraries except SL150)

1. **Use the following command to create a v3 user:**

> **Note –** Because of the complexity of this command, it is recommended that you create it in a text file on your PC or workstation, and then copy and paste the command directly into the CLI command line. See "CLI Usage Tips" on page 15 for details.

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

> **Note –** For the SL3000 and SL8500, the user name and both passwords must be enclosed in single quotes. However, for the SL500, do not enclose the passwords in quotes, as they will be accepted as text.

> **Note –** Passwords must be at least eight characters in length. Type **`help snmp`** at the CLI command line for a list of valid characters.

Where:

- *name* is the name you want to assign to the SNMP user. All libraries monitored by a single STA server must have the same v3 user name. It is recommended that you create a new, unique user for this purpose.
- *auth_password* is the authorization password you want to assign
- *priv_password* is the privacy password you want to assign

### *SL3000 Example*

**Note –** The SL8500 display is similar.

```
SL3000> snmp addUser version v3 name 'STAsnmp' auth SHA
authPass 'authpwd1' priv DES privPass 'privpwd1'
   requestId
   requestId 12345
   Device 1,0,0,0,1
   Success true
   Done
   Failure Count 0
   Success Count 1
COMPLETED
```

### *SL500 Example*

```
SL500> snmp addUser version v3 name STAsnmp auth SHA authPass
authpwd1 priv DES privPass privpwd1
   requestId
   requestId 12345
   Device 1,0,0,0,1
   Success true
   Done
   Failure Count 0
   Success Count 1
COMPLETED
```

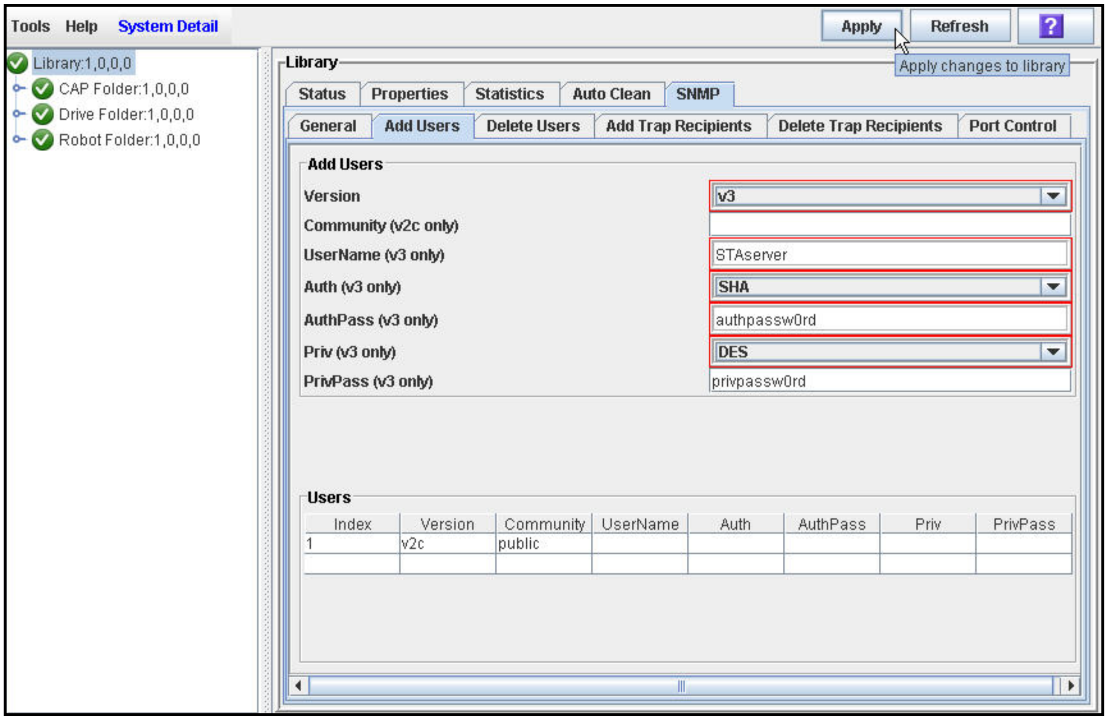
2. **List the SNMP users to verify that the v3 user has been added correctly.**

```
SL500> snmp listUsers
   requestId
   requestId 12345

   Attributes Auth      SHA
              Auth Pass *****
              Index     2
              Name      STAsnmp
              Priv      DES
              Priv Pass *****
              Version   v3
   Object     Snmp      snmp

   Attributes Community Public
              Index     1
              Version   v2c
   Object     Snmp      snmp

   Done
   Failure Count 0
   Success Count 1
COMPLETED
```

3. **Proceed to “Retrieve the Library SNMP Engine ID” on page 60.**

## ▼ With the SL Console (SL500 Libraries Only)

1. **Select System Detail > Library > SNMP > Add Users.**
2. **To add the SNMP v3 user, complete the Add Users tab as follows:**
   - **Version** – Select v3 from the menu.
   - **UserName** – Enter the name you want to assign to the SNMP user. All libraries monitored by a single STA server must have the same v3 user name. It is recommended that you create a new, unique user for this purpose.
   - **Auth** – Select SHA from the menu.
   - **AuthPass** – Enter the authorization password you want to assign.
   - **Priv** – Select DES from the menu.
   - **PrivPass** – Enter the privacy password you want to assign.



Add Users

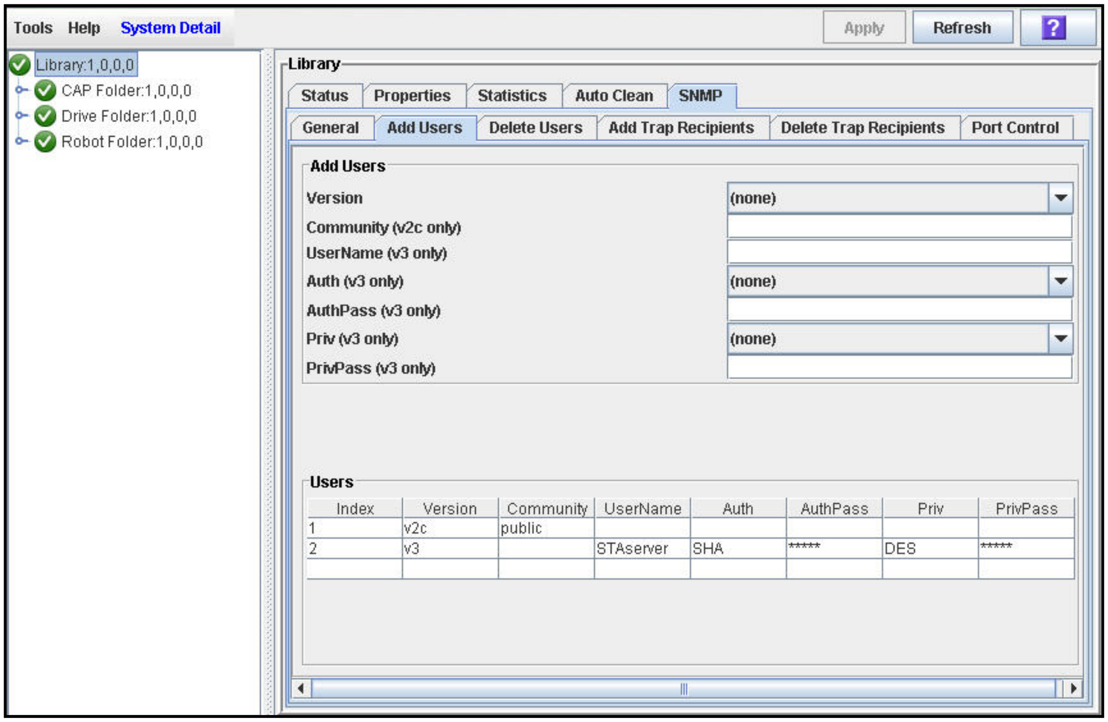
| | |
|---|---|
| Version | v3 |
| Community (v2c only) | |
| UserName (v3 only) | STAserver |
| Auth (v3 only) | SHA |
| AuthPass (v3 only) | authpassw0rd |
| Priv (v3 only) | DES |
| PrivPass (v3 only) | privpassw0rd |

Users

| Index | Version | Community | UserName | Auth | AuthPass | Priv | PrivPass |
|---|---|---|---|---|---|---|---|
| 1 | v2c | public | | | | | |

3. **Click Apply.**

   The user is added and the screen is updated.



Add Users

| | |
|---|---|
| Version | (none) |
| Community (v2c only) | |
| UserName (v3 only) | |
| Auth (v3 only) | (none) |
| AuthPass (v3 only) | |
| Priv (v3 only) | (none) |
| PrivPass (v3 only) | |

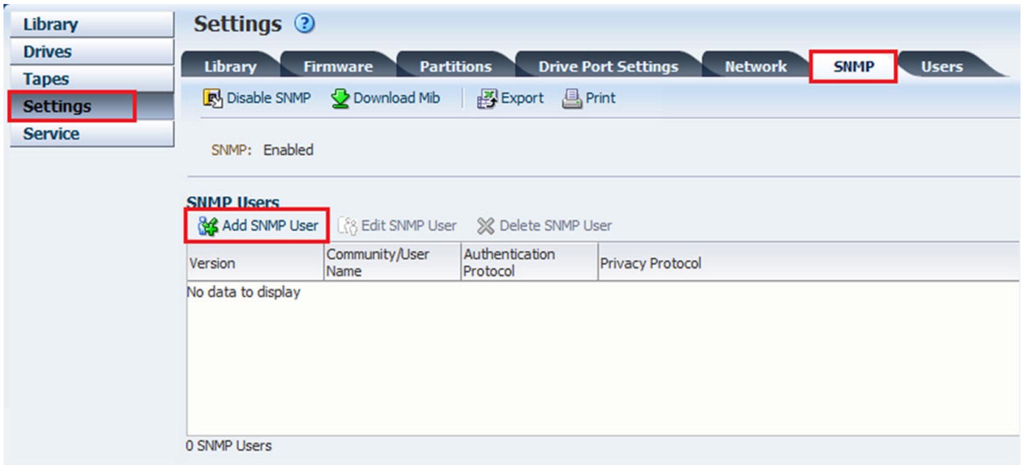
Users

| Index | Version | Community | UserName | Auth | AuthPass | Priv | PrivPass |
|---|---|---|---|---|---|---|---|
| 1 | v2c | public | | | | | |
| 2 | v3 | | STAserver | SHA | ***** | DES | ***** |

4. **Proceed to "Retrieve the Library SNMP Engine ID" on page 60.**

## ▼ With the SL150 User Interface

1. **Select Settings from the navigation bar on the left side of the interface.**
2. **Select the SNMP tab.**
3. **Under SNMP Users, select Add SNMP User.**



SNMP: Enabled

| Version | Community/User Name | Authentication Protocol | Privacy Protocol |
|---|---|---|---|
| No data to display | | | |

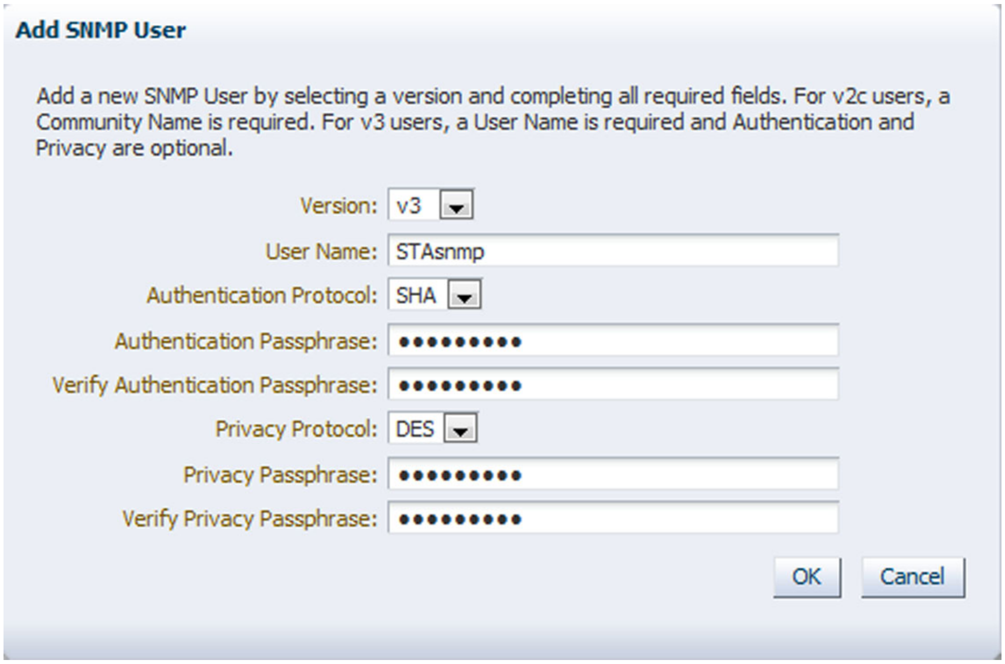
0 SNMP Users

4. **For Version, select v3, then complete the information as follows:**

   - **User Name** – Enter the name you want to assign to the SNMP user. All libraries monitored by a single STA server must have the same v3 user name. It is recommended that you create a new, unique user for this purpose.

- **Authentication Protocol** – Select SHA from the menu.
- **Authentication Passphrase** – Enter the authorization password you want to assign.
- **Verify Authentication Passphrase** – Re-type the passphrase.
- **Privacy Protocol** – Select DES from the menu.
- **Privacy Passphrase** – Enter the privacy password you want to assign.
- **Verify Privacy Passphrase** – Re-type the passphrase.

5. **Click OK.**



Add SNMP User

Add a new SNMP User by selecting a version and completing all required fields. For v2c users, a Community Name is required. For v3 users, a User Name is required and Authentication and Privacy are optional.

Version: v3
User Name: STAsnmp
Authentication Protocol: SHA
Authentication Passphrase: ●●●●●●●●●
Verify Authentication Passphrase: ●●●●●●●●●
Privacy Protocol: DES
Privacy Passphrase: ●●●●●●●●●
Verify Privacy Passphrase: ●●●●●●●●●

6. **Proceed to “Create an SNMP v3 Trap Recipient” on page 61.**

# ▼ Retrieve the Library SNMP Engine ID

**Note –** This procedure does not apply to the SL150 library.

Use this procedure to display the library SNMP engine ID, and then save it to a text file for use in "Create an SNMP v3 Trap Recipient" on page 61 and "Configure SNMP Connections With the Library" on page 84.

**Note –** If your library firmware is below the versions listed in "Ensure an SNMP v2c User" on page 49, you must have a v2c "public" user defined in order for the following command to successfully display the SNMP engine ID.

**Note –** You must use the CLI for this procedure.

## ▼ For SL3000 and SL8500 Libraries

1. **Display the library SNMP engine ID.**

```
SL3000> snmp engineId print
   engineID: 0x81031f88804b7e542f49701753
COMPLETED
```

2. **Copy and paste the displayed engine ID into a text file, and then save the file.**
3. **Proceed to "Create an SNMP v3 User" on page 55.**

## ▼ For SL500 Libraries

1. **Display the library SNMP engine ID.**

```
SL500> snmp engineId
snmp engineID:0x81031f88804b7e542f49701753
```

2. **Copy and paste the displayed engine ID into a text file, and then save the file.**
3. **Proceed to "Create an SNMP v3 User" on page 55.**

## ▼ Create an 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 –** Before performing this procedure, you must obtain the IP address of the STA server, which was established during the STA installation. For details, see the "Installing STA" chapter within the *StorageTek Tape Analytics Planning and Installation Guide*.

> **Note –** If you want 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.

> **Note –** The SNMP v3 trap recipient you create in this procedure must have the same name as the SNMP v3 user you created previously. See "Create an SNMP v3 User" on page 55.

> **Note –** For SL500 libraries, you can choose to perform this procedure with either the CLI or the SL Console. For SL3000 and SL8500 libraries, you must use the CLI. For SL150 libraries, you use the browser-based user interface.

### ▼ With the CLI (All libraries except SL150)

1. **Use the following command to create a v3 SNMP trap recipient:**

> **Note –** Because of the complexity of this command, it is recommended that you create it in a text file on your PC or workstation, and then copy and paste the command directly into the CLI command line. See "CLI Usage Tips" on page 15 for details.

> **Note –** For SL3000 and SL8500 libraries, do not include trap level 4. It is not supported by the SL3000 and SL8500 libraries.

**`snmp addTrapRecipient trapLevel 1,2,3,4,11,21,25,27,41,45, 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*

> **Note –** Trap levels must be entered individually, separated by commas (,).

> **Note –** For the SL3000 and SL8500 libraries, the user name and both passwords must be enclosed in single quotes. However, for the SL500 library, quotes are not required, and if you enter them they will be accepted as text.

> **Note –** Passwords must be at least eight characters in length. Type **`help snmp`** at the CLI command line for a list of valid characters.

Where:

- *STA_server_IP* is the IP address of the STA server.
- *recipient_name* is the SNMP user name you created in the previous procedure, "Create an SNMP v3 User" on page 55.

- *auth_password* is the authorization password you created in "Create an SNMP v3 User" on page 55.
- *priv_password* is the privacy password you created in "Create an SNMP v3 User" on page 55.
- *library_engineID* is the library engine ID you displayed in "Retrieve the Library SNMP Engine ID" on page 60. You MUST include the 0x prefix.

  **Note –** If you saved the engine ID in a text file, you can copy and paste it directly into this command.

### SL3000 Example

**Note –** The SL8500 display is similar.

**Note –** Do not include trap level 4. It is not supported by the SL3000 and SL8500 libraries.

```
SL3000> snmp addTrapRecipient trapLevel
1,2,3,11,21,25,27,41,45,61,63,65,81,85,100 host 10.80.125.23
version v3 name 'STAsnmp' auth SHA authPass 'authpwd1' priv DES
privPass 'privpwd1' engineId 0x81031f88804b7e542f49701753
   requestId
   requestId 12345
   Device 1,0,0,0,0
   Success true
   Done
   Failure Count 0
   Success Count 1
COMPLETED
```

### SL500 Example

```
SL500> snmp addTrapRecipient trapLevel
1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100 host
10.80.125.23 version v3 name STAsnmp auth SHA authPass authpwd1
priv DES privPass privpwd1 engineId
0x81031f88804b7e542f49701753
   requestId
   requestId 12345
   Device 1,0,0,0
   Success true
   Done
   Failure Count 0
   Success Count 1
COMPLETED
```

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

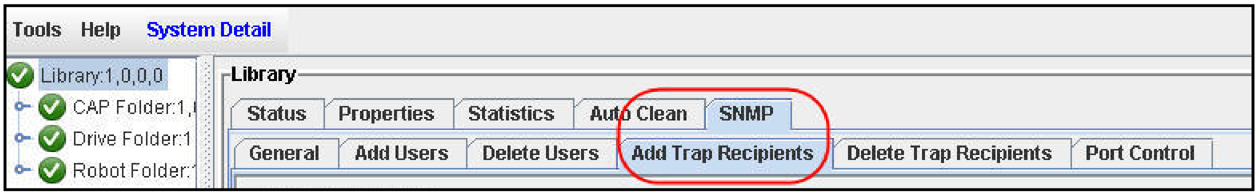
```
SL500> snmp listTrapRecipients
  requestId
  requestId 12345
  Attributes Auth       SHA
             Auth Pass  *****
             Engine Id  0x81031f88804b7e542f49701753
             Host       10.80.175.121
             Index      1
             Name       STAsnmp
             Port       162
             Priv       DES
             Priv Pass  *****
            Trap Level 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100
             Version    v3
   Object    Snmp       snmp
   Done
   Failure Count 0
   Success Count 1
COMPLETED
```

3. **Proceed as follows:**

   - If you are configuring an SL500 library, then proceed to "Set the SL500 Volume Label Format" on page 68.
   - If you are configuring an SL3000 or SL8500 library that does not use the Dual TCP/IP feature, proceed to "Set the Drive Cleaning Warning" on page 71.
   - If you want 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. Then, proceed to "Set the Drive Cleaning Warning" on page 71.

## ▼ With the SL Console (SL500 libraries only)

1. **Select System Detail > Library > SNMP > Add Trap Recipients.**



2. **To add the trap recipient, complete the Trap Recipients screen fields as follows:**

   - **Host** – Enter the IP address of the STA server.
   - **TrapLevel** – Specify the trap levels that the library should send to STA: `1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100`

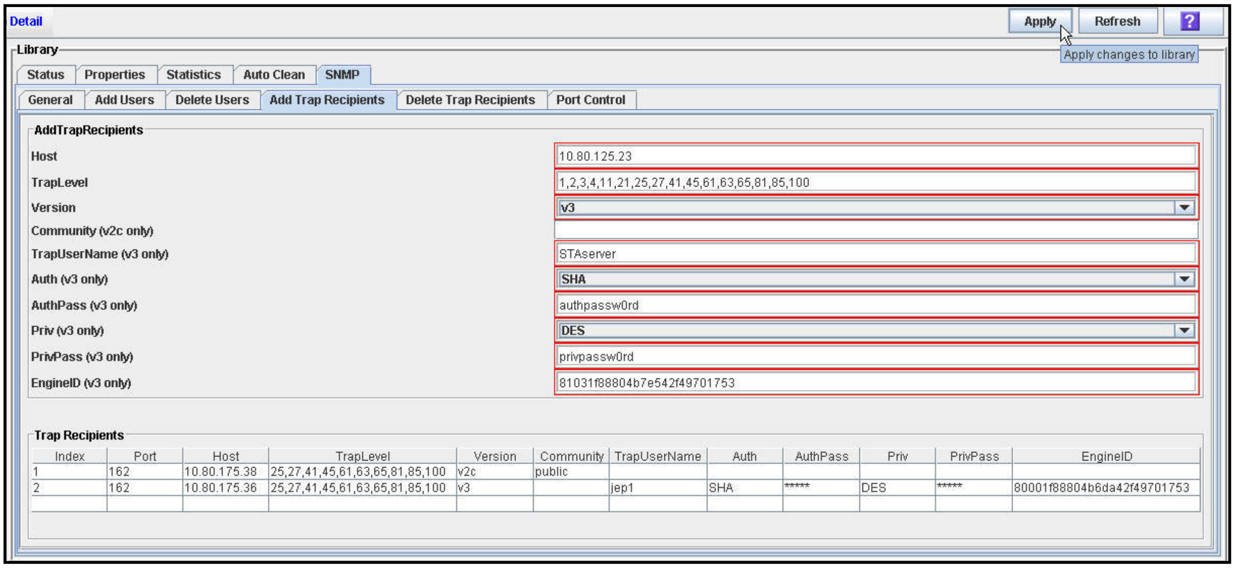
     **Note –** Trap levels must be entered individually, separated by commas (,).

   - **Version** – Select v3 from the menu.

- **TrapUserName** – Enter the SNMP user name you created in the previous procedure, "Create an SNMP v3 User" on page 55.
- **Auth** – Select SHA from the menu.
- **AuthPass** – Enter the authorization password you created in "Create an SNMP v3 User" on page 55.
- **Priv** – Select DES from the menu.
- **PrivPass** – Enter the privacy password you created in "Create an SNMP v3 User" on page 55.
- **EngineID** – Enter the library engine ID you displayed in "Create an SNMP v3 User" on page 55. Do NOT include the 0x prefix.

  **Note –** Future SL500 firmware may require the 0x prefix.

  **Note –** If you saved the engine ID in a text file, you can copy and paste it directly into this field.



AddTrapRecipients

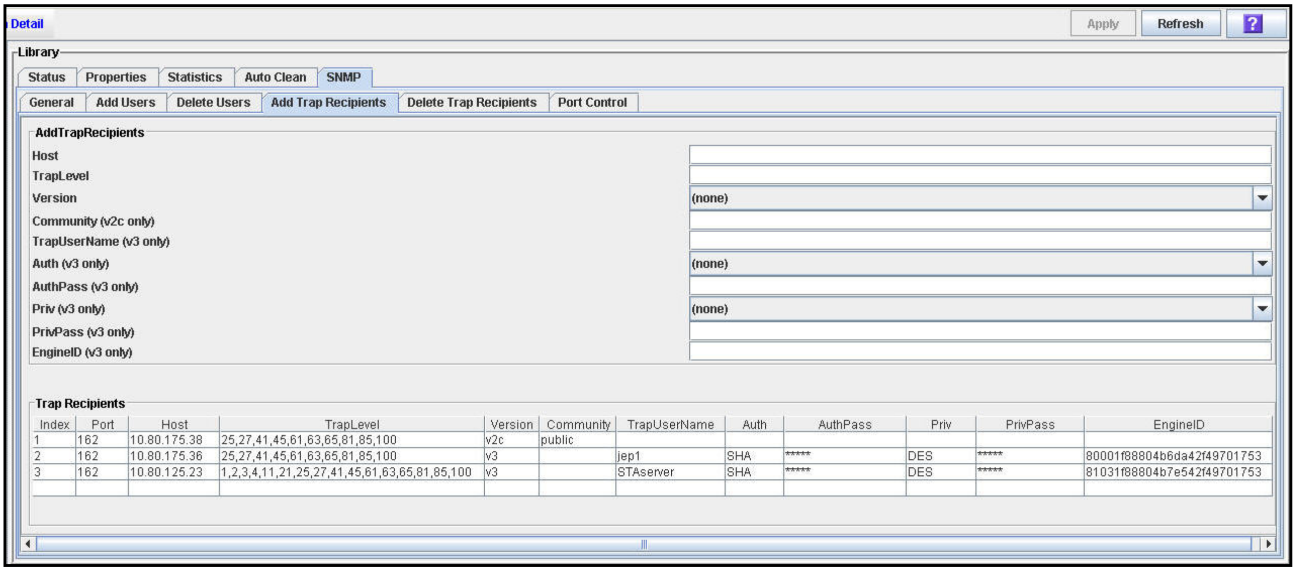
| | |
|---|---|
| Host | 10.80.125.23 |
| TrapLevel | 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100 |
| Version | v3 |
| Community (v2c only) | |
| TrapUserName (v3 only) | STAserver |
| Auth (v3 only) | SHA |
| AuthPass (v3 only) | authpassw0rd |
| Priv (v3 only) | DES |
| PrivPass (v3 only) | privpassw0rd |
| EngineID (v3 only) | 81031f88804b7e542f49701753 |

Trap Recipients

| Index | Port | Host | TrapLevel | Version | Community | TrapUserName | Auth | AuthPass | Priv | PrivPass | EngineID |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 162 | 10.80.175.38 | 25,27,41,45,61,63,65,81,85,100 | v2c | public | | | | | | |
| 2 | 162 | 10.80.175.36 | 25,27,41,45,61,63,65,81,85,100 | v3 | | jep1 | SHA | ***** | DES | ***** | 80001f88804b6da42f49701753 |

3. **Click Apply.**

   The trap recipient is added and the screen is updated.



AddTrapRecipients

| | |
|---|---|
| Host | |
| TrapLevel | |
| Version | (none) |
| Community (v2c only) | |
| TrapUserName (v3 only) | |
| Auth (v3 only) | (none) |
| AuthPass (v3 only) | |
| Priv (v3 only) | (none) |
| PrivPass (v3 only) | |
| EngineID (v3 only) | |

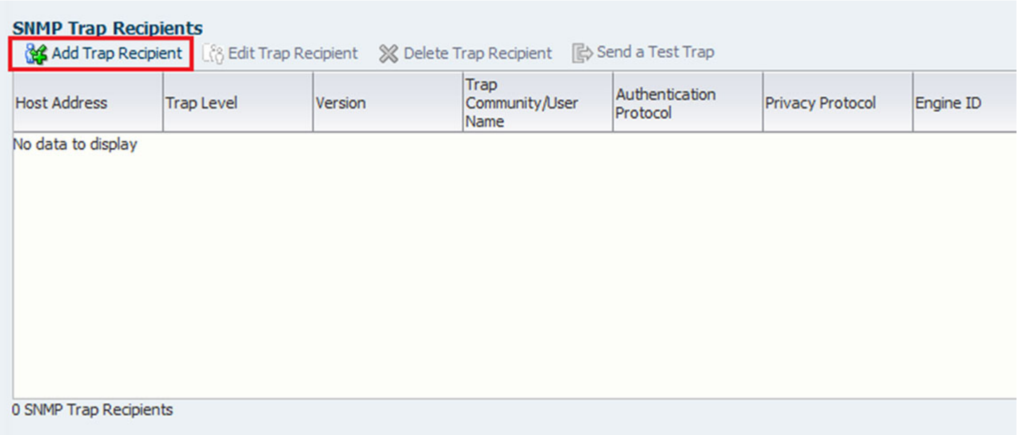
Trap Recipients

| Index | Port | Host | TrapLevel | Version | Community | TrapUserName | Auth | AuthPass | Priv | PrivPass | EngineID |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 162 | 10.80.175.38 | 25,27,41,45,61,63,65,81,85,100 | v2c | public | | | | | | |
| 2 | 162 | 10.80.175.36 | 25,27,41,45,61,63,65,81,85,100 | v3 | | jep1 | SHA | ***** | DES | ***** | 80001f88804b6da42f49701753 |
| 3 | 162 | 10.80.125.23 | 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100 | v3 | | STAserver | SHA | ***** | DES | ***** | 81031f88804b7e542f49701753 |

4. **Proceed to "Set the SL500 Volume Label Format" on page 68.**

## ▼ With the SL150 User Interface

1. **Select Settings from the navigation bar on the left side of the interface.**
2. **Select the SNMP tab.**
3. **Under SNMP Trap Recipients, select Add Trap Recipient.**



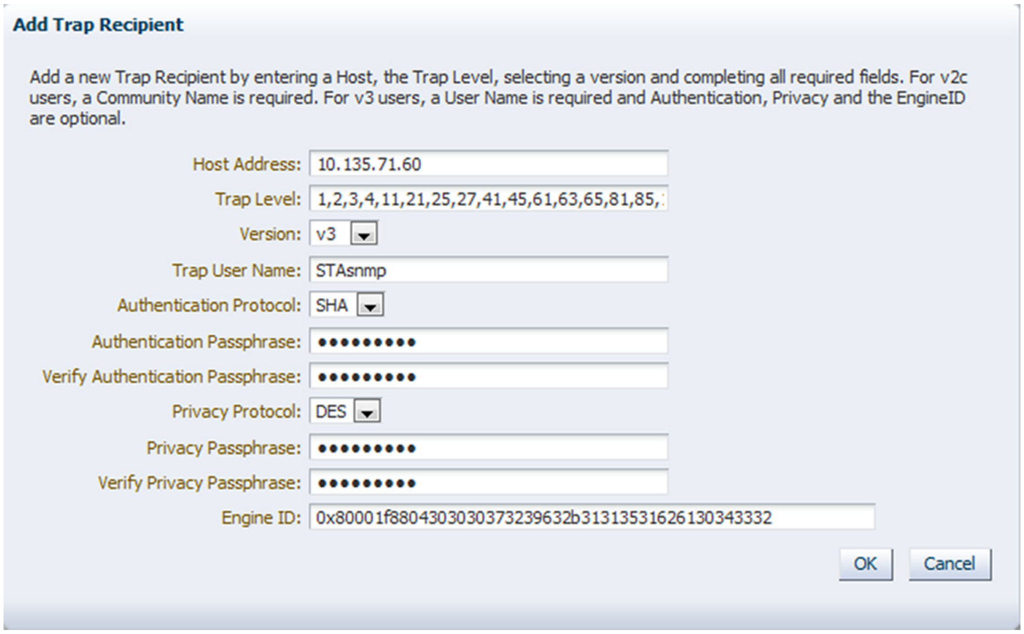
| Host Address | Trap Level | Version | Trap Community/User Name | Authentication Protocol | Privacy Protocol | Engine ID |
|---|---|---|---|---|---|---|
| No data to display | | | | | | |

0 SNMP Trap Recipients

4. **To add the trap recipient, complete the Add Trap Recipient fields as follows:**
   - **Host Address** – Enter the IP address of the STA server.
   - **Trap Level** – Specify the trap levels that the library should send to STA: `1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100`

     **Note –** Trap levels must be entered individually, separated by commas (,).
   - **Version** – Select v3.

- **Trap User Name** – Enter the SNMP user name you created in the previous procedure, "Create an SNMP v3 User" on page 55.
- **Authentication Protocol** – Select SHA.
- **Authentication Passphrase** – Enter the authorization password you created in "Create an SNMP v3 User" on page 55.
- **Verify Authentication Passphrase** – Re-type the passphrase.
- **Privacy Protocol** – Select DES.
- **Privacy Passphrase** – Enter the privacy password you created in "Create an SNMP v3 User" on page 55.
- **Verify Privacy Passphrase** – Re-type the passphrase.
- **Engine ID** – This field will auto-populate. Do not modify the value.



**Add Trap Recipient**

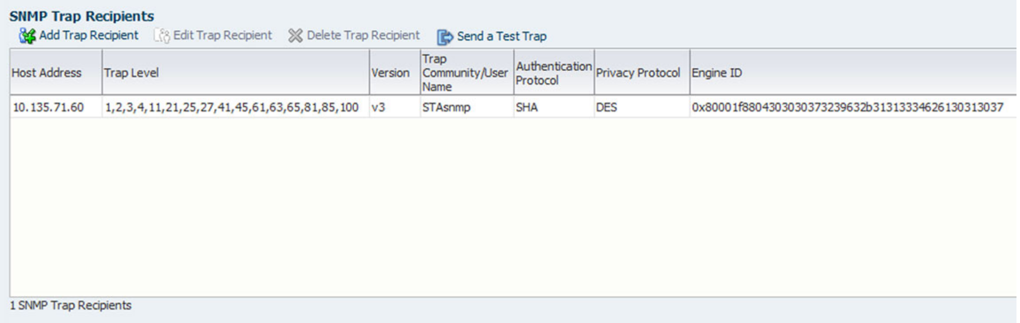
Add a new Trap Recipient by entering a Host, the Trap Level, selecting a version and completing all required fields. For v2c users, a Community Name is required. For v3 users, a User Name is required and Authentication, Privacy and the EngineID are optional.

| | |
|---|---|
| Host Address: | 10.135.71.60 |
| Trap Level: | 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,: |
| Version: | v3 |
| Trap User Name: | STAsnmp |
| Authentication Protocol: | SHA |
| Authentication Passphrase: | ●●●●●●●●● |
| Verify Authentication Passphrase: | ●●●●●●●●● |
| Privacy Protocol: | DES |
| Privacy Passphrase: | ●●●●●●●●● |
| Verify Privacy Passphrase: | ●●●●●●●●● |
| Engine ID: | 0x80001f8804303030373239632b313135316261303433332 |

5. **Click OK.**

   The trap recipient is added and the screen is updated.

   > **Note –** Do not click the "Send a Test Trap" button, as test traps are not supported by STA.



**SNMP Trap Recipients**

| Host Address | Trap Level | Version | Trap Community/User Name | Authentication Protocol | Privacy Protocol | Engine ID |
|---|---|---|---|---|---|---|
| 10.135.71.60 | 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100 | v3 | STAsnmp | SHA | DES | 0x80001f8804303030373239632b3131333462613031303 7 |

1 SNMP Trap Recipients

6. **Proceed to "Set the SL150 Volume Label Format" on page 70.**

# ▼ Set the SL500 Volume Label Format

**Note –** This procedure applies only to the SL500 library.

Use these two CLI procedures to ensure that volume serial numbers (VSNs) are formatted correctly in SNMP data sent to the STA server. This allows STA to correctly process library exchange data. See "Volume Label Formatting" on page 23 for details.

**Caution –** If these parameters are not set properly, VSNs will be formatted incorrectly for STA. This will cause 1) exchanges processing to be blocked, 2) superfluous attempts by STA to get the latest media data from the library, and 3) irreversible, eight-character VSN records to appear on the Media - Overview screen whenever the "Show Removed Media" preference is set.

## ▼ Set the Host Label Orientation

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
SL500>
```

2. **"Host" 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.
OK
SL500>
```

3. **Display the setting again to verify that 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
SL500>
```

## ▼ Set STA Mode

1. **Display the current setting of the STAconfig flag.**

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

2. **STA mode must be enabled. To enable the flag, use the following command:**

```
SL500> staConfig on
SL500>
```

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

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

4. **You have finished configuring the SL500 library for STA and can go to Chapter 2, Configuring SNMP in the STA Application" on page 75.**

## ▼ Set the SL150 Volume Label Format

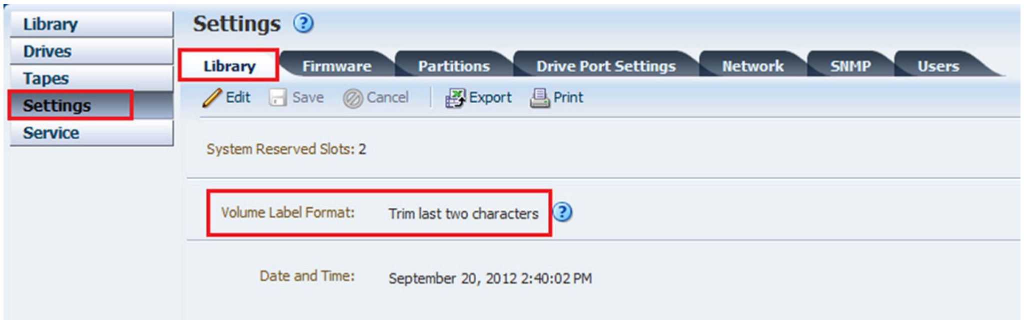
**Note –** This procedure applies only to the SL150 library.

Use this procedure to set the volume label format properly on an SL150 library. This ensures that volume serial numbers (VSNs) are formatted correctly in SNMP data sent to the STA server so that STA can correctly process library exchange data. See "Volume Label Formatting" on page 23 for details.

**Caution –** If the volume label format is not set properly, VSNs will be formatted incorrectly for STA. This will cause 1) exchanges processing to be blocked, 2) superfluous attempts by STA to get the latest media data from the library, and 3) irreversible, eight-character VSN records to appear on the Media - Overview screen whenever the "Show Removed Media" preference is set.

1. **Select Settings from the navigation bar on the left side of the interface.**
2. **Select the Library tab.**

   Volume Label Format should be set to "Trim last two characters". If it is not, proceed to the next step.

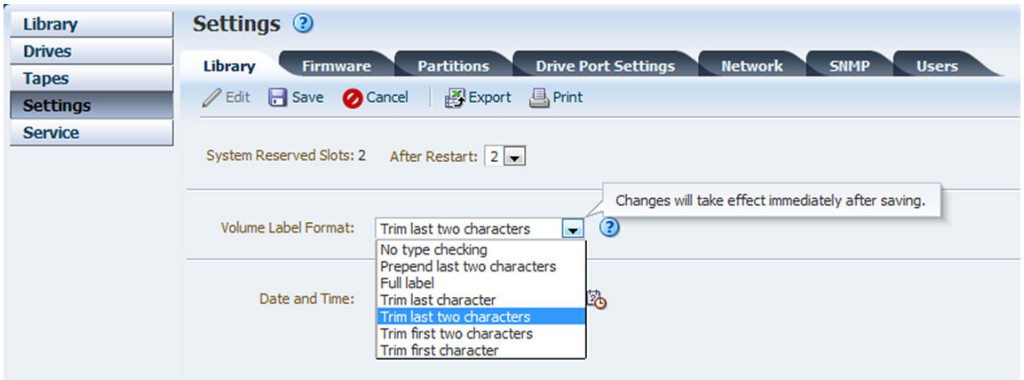


System Reserved Slots: 2

Volume Label Format: Trim last two characters

Date and Time: September 20, 2012 2:40:02 PM

3. **Select the Edit button.**
4. **Set Volume Label Format to "Trim last two characters".**
5. **Click Save.**



System Reserved Slots: 2 After Restart: 2

Changes will take effect immediately after saving.

Volume Label Format: Trim last two characters

Date and Time:

## ▼ Set the Drive Cleaning Warning

**Note –** This procedure applies only to the SL3000 and SL8500 libraries.

Use this optional CLI procedure to check the current setting of the drive cleaning warning flag on the library and change it if necessary. See "Drive Cleaning Warning" on page 24 for details.

1. **Use the following command to display the current setting of the drive cleaning warning flag:**

```
SL3000> cleaning driveWarning get
   requestId
   requestId 12345
   Attributes
   Object     Drive Cleaning Warning true
   Done
COMPLETED
```

2. **If you want to set the flag to "off", use the following command:**

```
SL3000> cleaning driveWarning set off
   requestId
   requestId 12345
   Attributes
   Object     Success true
   Done
COMPLETED
```

3. **Proceed as follows:**

   - For SL3000 libraries, you have finished configuring the library for STA and can proceed to Chapter 2, Configuring SNMP in the STA Application" on page 75.
   - For SL8500 libraries, proceed to "Ensure the Correct Library Complex ID" on page 72.

## ▼ Ensure the Correct Library Complex ID

**Note –** This procedure applies only to the SL8500 library.

Use this procedure to ensure the correct library complex ID information for each SL8500 library. See "Library Complex IDs" on page 25 for details.

**Caution –** The Oracle Service Delivery Platform (SDP) also uses complex IDs for tracking library data. If SDP is in use at your site, consult Oracle Service 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.

**Note –** You must perform this procedure from the CLI.

1. **For each SL8500 library that will be monitored by STA, use the following command to display the complex ID currently assigned:**

```
SL8500> config complexId print
   requestid
   requestid 12345
   Complex Id 3
   Done
   Failure Count 0
   Success Count 1
COMPLETED
```

2. **Compare the results, as follows:**

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

   If you need to change the complex ID of a standalone library, go to Step 3, below.

   **Caution –** If you need to change the complex ID of a library in an SL8500 multi-library complex, consult with your Oracle support representative. Do not continue with this procedure.

3. **Place the library offline, and wait for all transactions to complete. See the "Manual Operations" chapter of your library** *User's Guide* **for instructions.**

4. **Use the following command to change the complex ID of a standalone library:**

   **`config complexId set`** *complex_ID*

   Where:

   - *complex_ID* is the new complex ID; a number 1–253.

```
SL8500> config complexId set 5
   requestid
   requestid 12345
   Complex Id 5
   Success    true
   Done
   Failure Count 0
   Success Count 1
   Note: TCP/IP stack reset may take a few seconds
         after command completion.
COMPLETED
```

5. **Reboot the library to activate the change. See the "SL Console Diagnostics and Utilities" chapter of your library** *User's Guide* **for instructions.**

6. **You have finished configuring the SL8500 library for STA and can proceed to Chapter 2, Configuring SNMP in the STA Application" on page 75.**

2

# Configuring SNMP in the STA Application

After the libraries have been configured to enable them to send data to StorageTek Tape Analytics (STA) (as described in Chapter 1), STA must be configured to receive data from the libraries.

This chapter contains the following topics:

- "Configuration Process" on page 75
- "Configuration Troubleshooting" on page 93

## Configuration Process

You will use the following process to configure STA to receive SNMP data from one or more libraries. Once this process is complete, STA can begin monitoring the libraries. You perform Step 3 once for all libraries, and then Step 4 through Step 7 once for each library.

> **Note –** If you are configuring multiple library connections at once, it is recommended that you complete Step 4 for all libraries before proceeding to Step 5, and then complete Step 5 for all libraries before proceeding to Step 6. This will minimize potential disruption to the libraries from SNMP connection tests and data collections.

1. "Verify SNMP Communications With the Library" on page 76.
2. "Log In to the STA User Interface" on page 78.
3. "Configure SNMP Client Settings for STA" on page 80
4. "Configure SNMP Connections With the Library" on page 84
5. "Verify the Library is Operational" on page 87
6. "Test the SNMP Connection to the Library" on page 89
7. "Get the Latest Configuration Data From the Library" on page 91

After you complete this process, you will configure email notifications to be sent by STA. See Chapter 3, "Configuring Email Notifications" on page 99.

## ▼ Verify SNMP Communications With the Library

Use this procedure to verify that the STA server is able to communicate with the library using the SNMP protocol. This procedure verifies that UDP ports 161 and 162 have been enabled on all network nodes between the STA server and the library.

1. **Establish a terminal session with the STA server, and log in as root.**

   See your STA server administrator for login information.

2. **To ensure SNMP services are turned off (deconfigured) and stopped, perform the following:**

   a. **Deconfigure SNMP services:**

   ```
   # chkconfig snmpd off
   # chkconfig snmptrapd off
   ```

   b. **Stop SNMP services:**

   ```
   # service snmptrapd stop
   # service snmpd stop
   ```

   > **Note –** If you receive a "FAILED" error when executing the "service stop" commands, these SNMP services may already be stopped.

   c. **Stop and restart STA services:**

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

3. **At the Linux command prompt, use the following command to test the SNMP connection by querying the library SNMP agent on the library.**

   ```
   snmpget -v3 -u SNMP_user -a SHA -A auth_password-x DES
   -X priv_password -l authPriv library_IP_addr
   1.3.6.1.4.1.1211.1.15.3.1.0
   ```

   > **Note –** To ensure the snmpget utility is available, see the "Ensure Availability of net-snmp-utils" section within the *StorageTek Tape Analytics Planning and Installation Guide*.

   Where:

   - *SNMP_user* is the SNMP user you created in "Create an SNMP v3 User" on page 55.
   - **SHA** indicates the authentication protocol.
   - *auth_password* is the authorization password you assigned in "Create an SNMP v3 User" on page 55.
   - **DES** indicates the privacy protocol.
   - *priv_password* is the privacy password you assigned in "Create an SNMP v3 User" on page 55.
   - **authPriv** indicates that authentication with privacy is performed on the command.
   - *library_IP_addr* is the IP address of the public port on the library, as follows:

  - For SL500 libraries, this is always the 1B port; see “Retrieve the Library IP Address” on page 36.
  - For SL3000 and SL8500 libraries, there may be multiple ports you want to test, depending on whether the Dual TCP/IP and/or Redundant Electronics features are activated on the library. See “Retrieve SL3000 or SL8500 IP Addresses” on page 36 for details. If there are multiple ports, you need to run this command once 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; this entry is the same for all library models.

### *Example of a Successful Command*

If the command displays the library model (for example, SL8500), this confirms the v3 user information and that all routes in the network between the library and the server on which STA is installed have ports 161 and 162 open.

```
# snmpget -v3 -u STAsnmp -a SHA -A authpwd1 -x DES -X privpwd1
-l authPriv 10.80.123.20 1.3.6.1.4.1.1211.1.15.3.1.0
SNMPv2-SMI::enterprises.1211.1.15.3.1.0 = STRING: "SL8500"
```

### *Example of Unsuccessful Commands*

```
# snmpget -v3 -u STAsnmp -a SHA -A authpwd1 -x DES -X privpwd1
-l authPriv 10.80.456.17 1.3.6.1.4.1.1211.1.15.3.1.0
Timeout: No Response from 10.80.456.17.
#
# snmpget -v3 -u WrongUsr -a SHA -A authpwd1 -x DES -X WrongPwd
-l authPriv 10.80.456.17 1.3.6.1.4.1.1211.1.15.3.1.0
snmpget: Authentication failure (incorrect password, community
or key)
#
```

4. **If the command was successful, proceed to “Log In to the STA User Interface” on page 78. If the command was not successful, contact your network administrator or Oracle support representative. You can also view the troubleshooting information in “Troubleshoot an Unsuccessful SNMP Connection” on page 93. You may need to troubleshoot issues with packet routing between the library and the STA server.**

## ▼ Log In to the STA User Interface

Use this procedure to start an STA session. Before using this procedure, you must verify that your computer and browser are configured correctly. For details, refer to the "Getting Started" chapter of the *StorageTek Tape Analytics User Interface Guide*.

1. **Start a supported Web browser on your computer.**

2. **In the Location Bar or Address field, enter the URL of the STA server.**

   The URL uses one of the following formats:

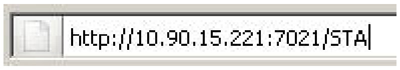
   - **`http://`***local_host_name***`:`***port_number***`/STA`**
   - **`https://`***local_host_name***`:`***port_number***`/STA`**

   Where:

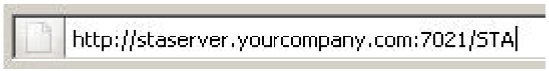
   - *local_host_name* is the IP address or fully qualified DNS alias of the STA server.
   - *port_number* is the port ID of the STA application.

     **Note –** The host name and port number were established during STA installation. For details, see the "Installing STA" chapter within the *StorageTek Tape Analytics Planning and Installation Guide*.

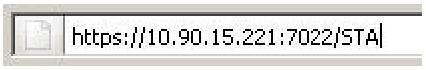
   Following are examples of each format.



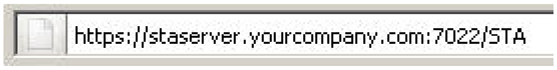
http://10.90.15.221:7021/STA



http://staserver.yourcompany.com:7021/STA

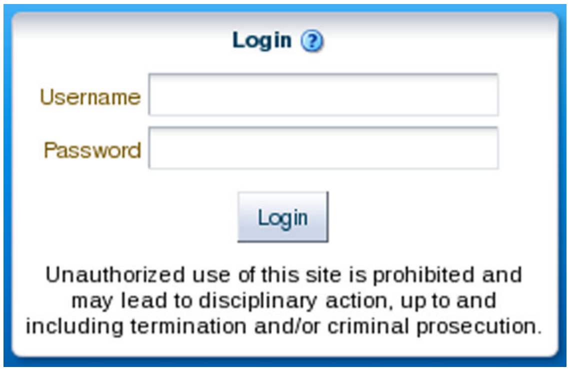


https://10.90.15.221:7022/STA



https://staserver.yourcompany.com:7022/STA

   The **Login** screen appears.



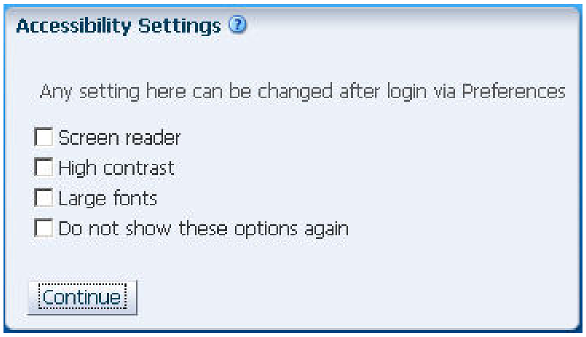
Unauthorized use of this site is prohibited and may lead to disciplinary action, up to and including termination and/or criminal prosecution.

3. **Enter your username and password.**

   **Note –** The local WebLogic STA user name and password were established during STA installation. For details, see the "Installing STA" chapter within the *StorageTek Tape Analytics Planning and Installation Guide*.

4. **Click Login.**

   Depending on the preference settings for your username, the Accessibility Settings dialog box may appear.



Accessibility Settings

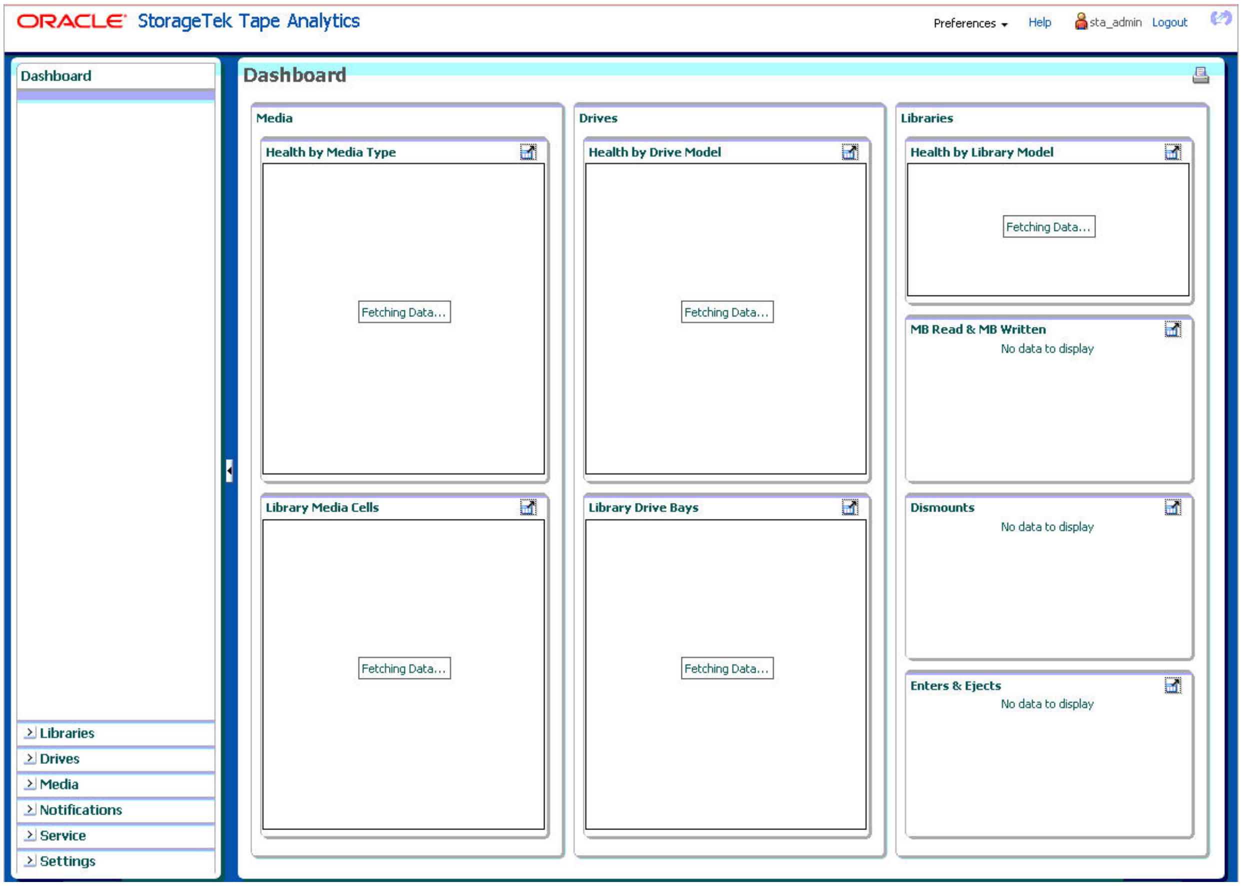
Any setting here can be changed after login via Preferences

□ Screen reader
□ High contrast
□ Large fonts
□ Do not show these options again

5. **Complete the Accessibility Settings dialog box, if applicable. See “Modify Accessibility Preferences” in the** *STA User Interface Guide* **for details on completing this dialog box.**

6. **Click Continue.**

   The Dashboard appears.



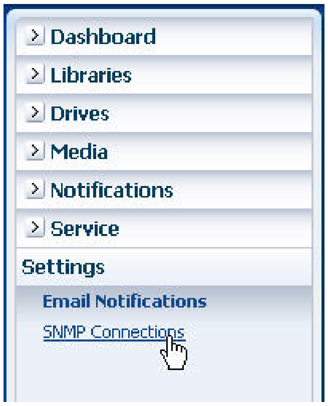
## ▼ Configure SNMP Client Settings for STA

Use this procedure to configure STA to receive SNMP data from one or more libraries. You need to create one client entry for your site.

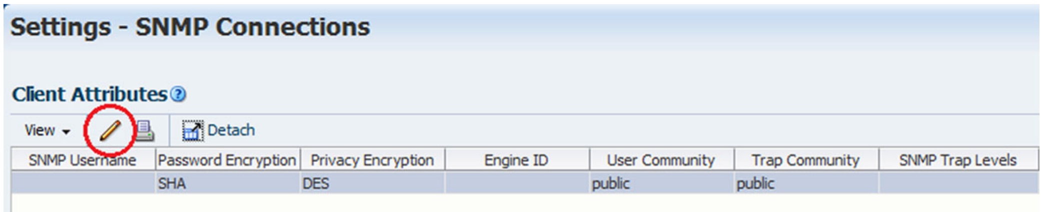
To perform this procedure, you need the following SNMP v3 user information you previously created for the library. See "Create an SNMP v3 User" on page 55 for details.

- SNMP v3 user name. This must be the same on all libraries monitored by STA.
- Connection authorization password.
- Privacy password.

1. **In the Navigation Bar, select Settings > SNMP Connections.**



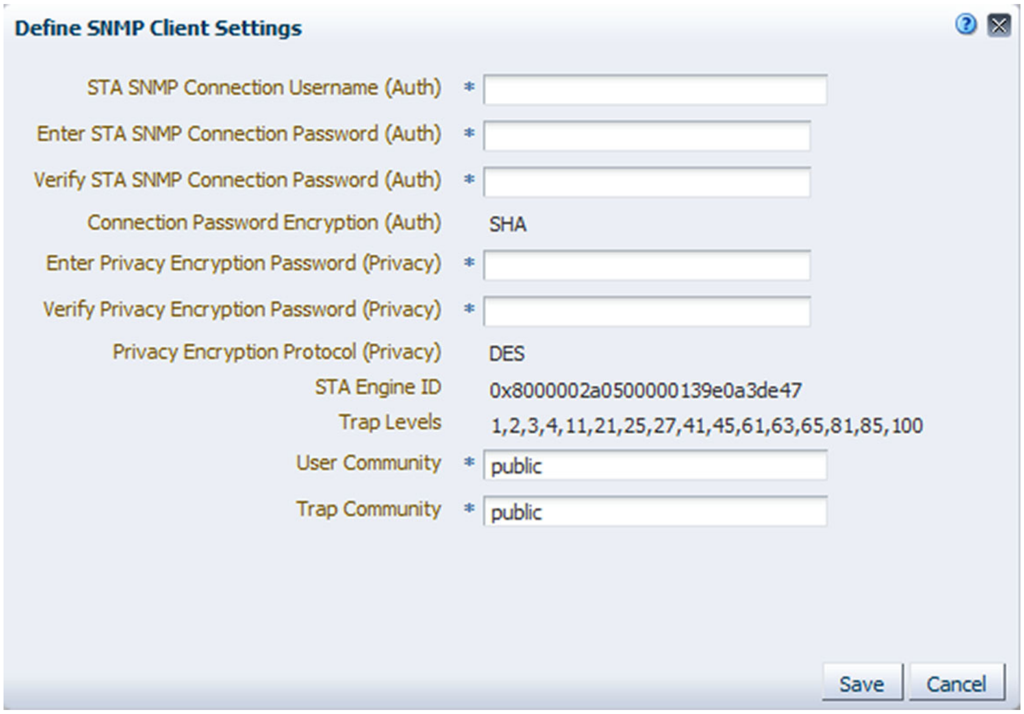
2. **In the Client Attributes table, select the empty table row. In the toolbar, click Edit.**



| SNMP Username | Password Encryption | Privacy Encryption | Engine ID | User Community | Trap Community | SNMP Trap Levels |
|---|---|---|---|---|---|---|
|  | SHA | DES |  | public | public |  |

The Define SNMP Client Settings dialog box appears. Before completing the dialog box, note the following:

- If the STA application will be monitoring only libraries configured for v3 communication, fill out all fields as specified in the following step. However, Trap Community can be left set to the default of "public", as this field will not be used by STA for v3 communications.
- If the STA application will be monitoring a mix of libraries configured for both v3 and v2c communication, fill out all fields as specified in the following step.
- If the STA application will be monitoring only libraries configured for v2c communication, you must still fill out all fields as specified in the following step — even those fields applicable to v3 communication.



Define SNMP Client Settings

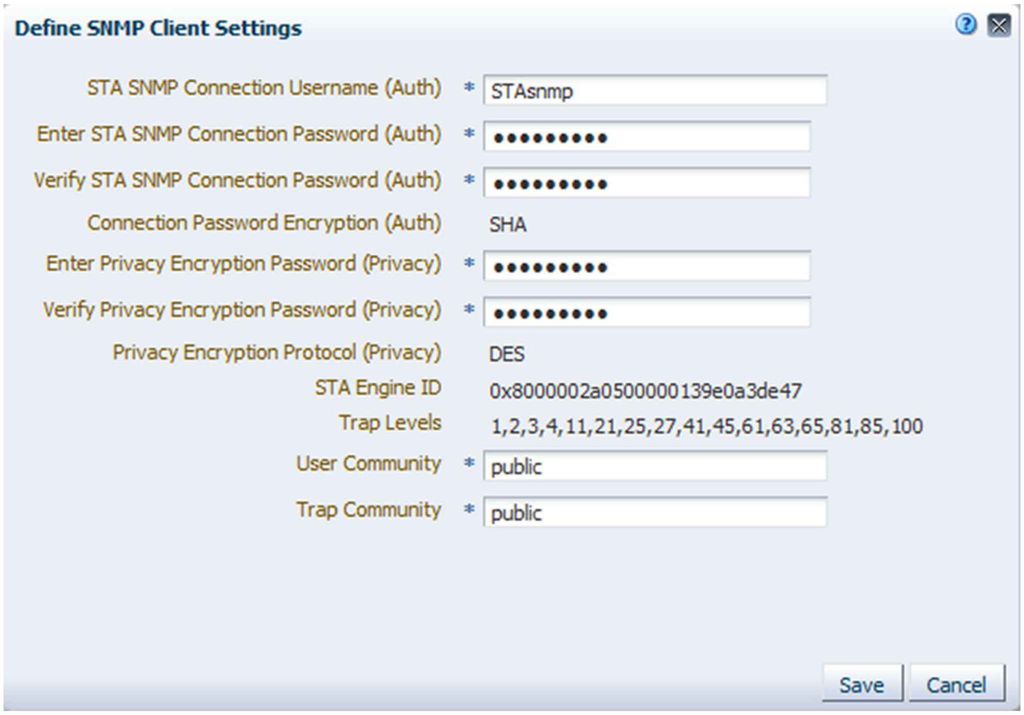
| | | |
|---|---|---|
| STA SNMP Connection Username (Auth) | * | |
| Enter STA SNMP Connection Password (Auth) | * | |
| Verify STA SNMP Connection Password (Auth) | * | |
| Connection Password Encryption (Auth) | | SHA |
| Enter Privacy Encryption Password (Privacy) | * | |
| Verify Privacy Encryption Password (Privacy) | * | |
| Privacy Encryption Protocol (Privacy) | | DES |
| STA Engine ID | | 0x8000002a0500000139e0a3de47 |
| Trap Levels | | 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100 |
| User Community | * | public |
| Trap Community | * | public |

3. **Complete the dialog box as follows.**

   - **STA SNMP Connection Username (Auth)** – Enter the SNMP v3 user name you created on the library.
   - **Enter STA SNMP Connection Password (Auth)** – Enter the connection authorization password you created for the SNMP v3 user on the library.
   - **Verify STA SNMP Connection Password (Auth)** – Re-type the connection password. An error message will be displayed if the two passwords do not match.
   - **Enter Privacy Encryption Password (Privacy)** – Enter the privacy encryption password you created for the SNMP v3 user on the library.
   - **Verify Enter Privacy Encryption Password (Privacy)** – Re-type the privacy password. An error message will be displayed if the two passwords do not match.
   - **User Community** – This field is only used by STA if v2c is required for the initial handshake with the library, or if v2c will be used for STA communication. The default setting is “public”, but can be changed to match the v2c user community specified on the library. The field cannot be blank. For more information regarding when a v2c user is required on the library, see “Ensure an SNMP v2c User” on page 49.
   - **Trap Community** – This field is only used by STA if v2c will be used for communication with the library. The default setting is “public”, but can be changed to match the v2c trap recipient community specified on the library. The field cannot be blank. For information on configuring libraries to use v2c instead of v3, see Appendix A, “Configuring SNMP v2c Mode”.

The following fields are display-only.

- **Connection Password Encryption (Auth)** – Encryption technique for storing the connection password. This is always SHA (Secure Hash Algorithm).
- **Privacy Encryption Protocol (Privacy)** – Encryption technique for the SNMP privacy mechanism. This is always DES (Data Encryption Standard).
- **STA Engine ID** – Globally unique SNMP engine ID for STA. This is assigned by STA and is distinct from the library engine ID provided by each library. Both are required to ensure secure communications.
- **Trap Levels** – List of all the SNMP traps that STA can process. This does not necessarily mean that these traps have been configured on the library; you must verify this on the library. See "Create an SNMP v3 Trap Recipient" on page 61 for details.

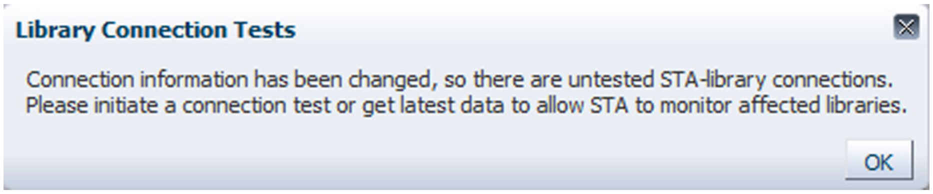


**Define SNMP Client Settings**

| | | |
|---|---|---|
| STA SNMP Connection Username (Auth) | * | STAsnmp |
| Enter STA SNMP Connection Password (Auth) | * | ●●●●●●●●● |
| Verify STA SNMP Connection Password (Auth) | * | ●●●●●●●●● |
| Connection Password Encryption (Auth) | | SHA |
| Enter Privacy Encryption Password (Privacy) | * | ●●●●●●●●● |
| Verify Privacy Encryption Password (Privacy) | * | ●●●●●●●●● |
| Privacy Encryption Protocol (Privacy) | | DES |
| STA Engine ID | | 0x8000002a0500000139e0a3de47 |
| Trap Levels | | 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100 |
| User Community | * | public |
| Trap Community | * | public |

4. **Click Save.**

   An information message appears, reminding you that a library connection test is required whenever you add or modify library connections. You will perform a connection test later, after defining the library connection information.

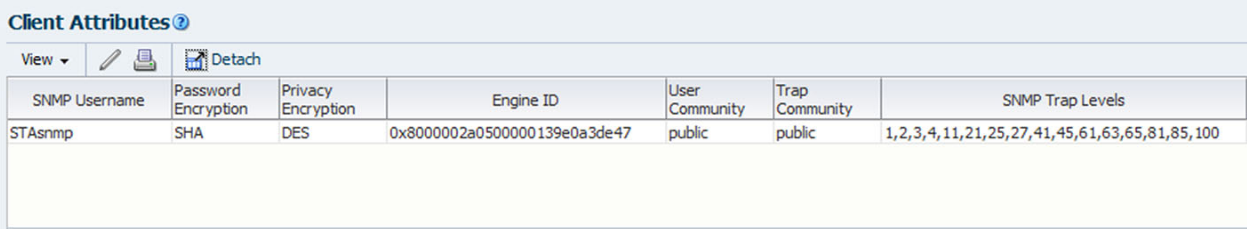


**Library Connection Tests**

Connection information has been changed, so there are untested STA-library connections. Please initiate a connection test or get latest data to allow STA to monitor affected libraries.

5. **Click OK to dismiss the dialog box.**

   Your entry is added to the Client Attributes table.



| SNMP Username | Password Encryption | Privacy Encryption | Engine ID | User Community | Trap Community | SNMP Trap Levels |
|---|---|---|---|---|---|---|
| STAsnmp | SHA | DES | 0x8000002a0500000139e0a3de47 | public | public | 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100 |

6. **Proceed to "Configure SNMP Connections With the Library" on page 84.**

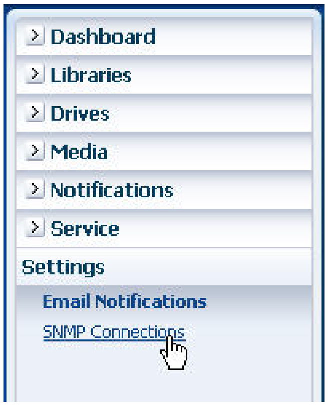
## ▼ Configure SNMP Connections With the Library

Use this procedure to configure SNMP connections between STA and a library. You perform this entire procedure for each library you want STA to monitor.

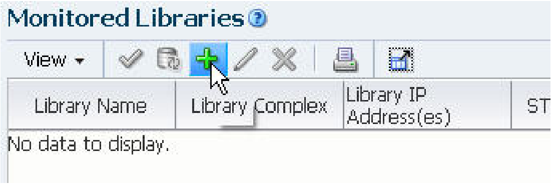
To perform this procedure, you need the following information:

- IP address of the STA server.
- IP address of the public port(s) on the library. You recorded this information in "Retrieve the Library IP Address" on page 36.

1. **In the Navigation Bar, select Settings > SNMP Connections.**



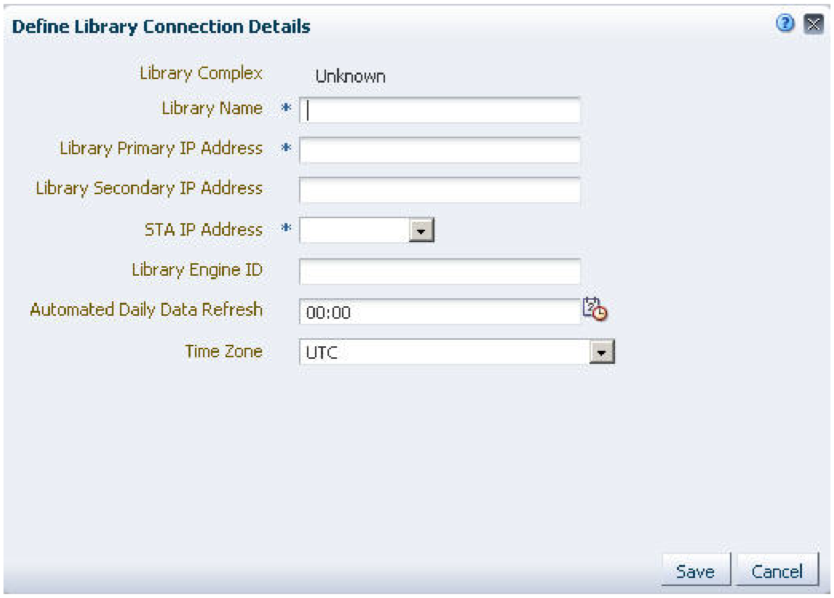
2. **In the Monitored Libraries toolbar, click Add.**



| Library Name | Library Complex | Library IP Address(es) | ST |
|---|---|---|---|

No data to display.

The Define Library Connection Details dialog box appears.



| | |
|---|---|
| Library Complex | Unknown |
| Library Name * | |
| Library Primary IP Address * | |
| Library Secondary IP Address | |
| STA IP Address * | |
| Library Engine ID | |
| Automated Daily Data Refresh | 00:00 |
| Time Zone | UTC |

3. **Complete the dialog box as follows:**

   - **Library Complex** – This is a display-only field and currently displays "Unknown". The complex ID will be automatically generated by STA after you have successfully retrieved the latest library configuration data. See "Get the Latest Configuration Data From the Library" on page 91 for details.
   - **Library Name** – Enter the name you want to assign to the library. This name will be used to identify the library throughout the STA user interface screens. You may want to use the library host name.
   - **Library Primary IP Address** – Enter the IP address of the primary public port on the library. For SL500 libraries, this is the 1B port. For SL3000 and SL8500 libraries, this is the 2B port. For SL150 libraries, this is Network Port 1. See "Retrieve the Library IP Address" on page 36.

     **Note –** For SL3000 and SL8500 libraries using the Redundant Electronics feature, this is the 2B port on the active controller card.

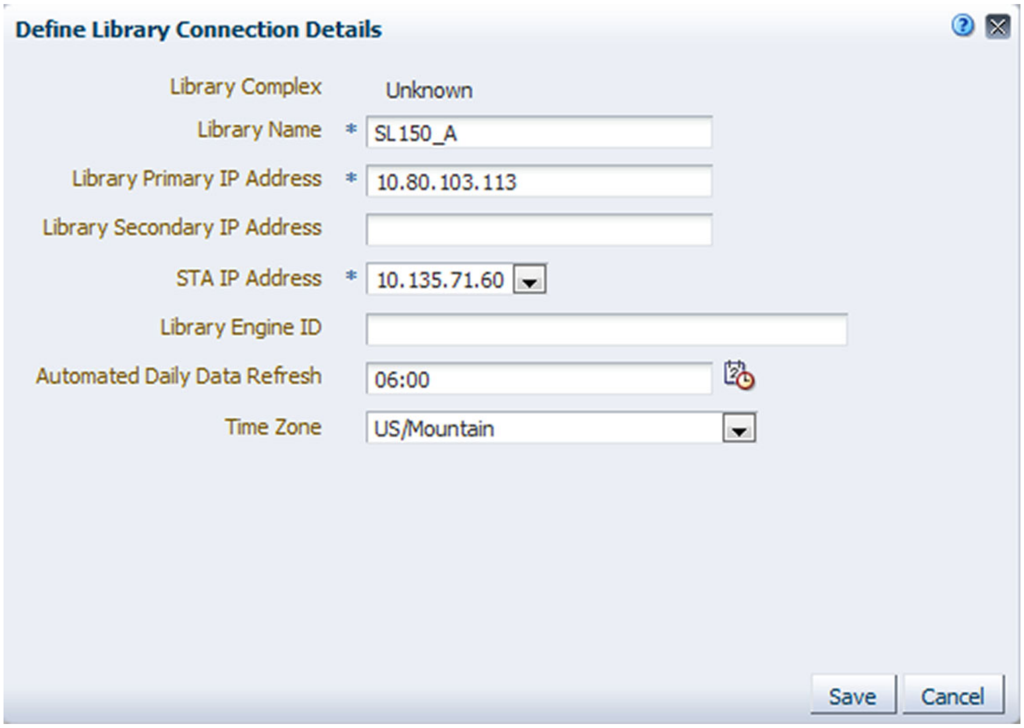
   - **Library Secondary IP Address** – For SL500 and SL150 libraries, this field does not apply and should be left blank. For SL3000 and SL8500 libraries, enter the secondary IP address you recorded in "Retrieve SL3000 or SL8500 IP Addresses" on page 36. Possible entries are as follows:
     - To configure STA to support Redundant Electronics, enter the IP address of the 2B port on the alternate (standby) controller card.
     - To configure STA to support Dual TCP/IP, enter the IP address of the 2A port on the active controller card.
     - For libraries with neither of these features, leave this field blank.
   - **STA IP Address** – In the menu, select the IP address of the STA server. The server address, in IPv4 format, is the only entry in the menu.
   - **Library Engine ID** – Leave this field blank. This is the unique SNMP engine ID of the library, and it is automatically provided by the library when the initial connection between STA and the library is made. See "Test the SNMP Connection to the Library" on page 89 for details.
   - **Automated Daily Data Refresh** – Enter the time of day when you want STA to collect the latest configuration data from the library. The data will be collected automatically every 24 hours at this time, local to the time zone you specify in the Time Zone field.

     The default is 00:00 (12:00 am). Use 24-hour time format for your entry (for example, 13:00 is 1:00 pm).

     **Note –** It is recommended that you choose a time period when there is typically lighter library usage, so the data collection does not conflict with other significant library activity.

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

   - **Time Zone** – In the menu, select the library's local time zone.



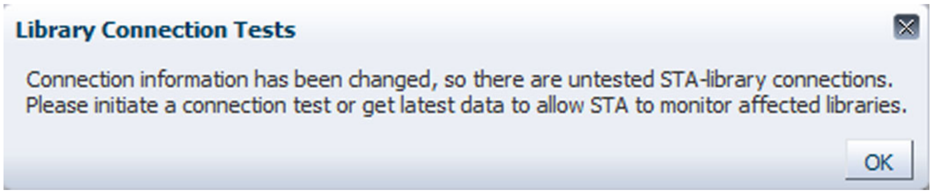
**Define Library Connection Details**

| | |
|---|---|
| Library Complex | Unknown |
| Library Name * | SL150_A |
| Library Primary IP Address * | 10.80.103.113 |
| Library Secondary IP Address | |
| STA IP Address * | 10.135.71.60 |
| Library Engine ID | |
| Automated Daily Data Refresh | 06:00 |
| Time Zone | US/Mountain |

4. **Click Save.**

   An information message appears, reminding you that a library connection test is required whenever you add or modify library connections. You will perform a connection test later, after verifying that the library is operational.

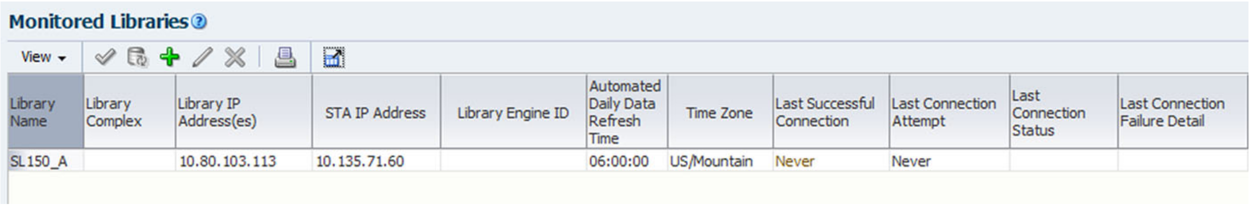
5. **Click OK to dismiss the message.**



**Library Connection Tests**

Connection information has been changed, so there are untested STA-library connections. Please initiate a connection test or get latest data to allow STA to monitor affected libraries.

Your entry is added to the Monitored Libraries table.



**Monitored Libraries**

| Library Name | Library Complex | Library IP Address(es) | STA IP Address | Library Engine ID | Automated Daily Data Refresh Time | Time Zone | Last Successful Connection | Last Connection Attempt | Last Connection Status | Last Connection Failure Detail |
|---|---|---|---|---|---|---|---|---|---|---|
| SL150_A | | 10.80.103.113 | 10.135.71.60 | | 06:00:00 | US/Mountain | Never | Never | | |

6. **Proceed to "Verify the Library is Operational" on page 87.**

# ▼ Verify the Library is Operational

Use this procedure to verify that a library is fully initialized and operational. You should use this procedure before performing either of the following procedures:

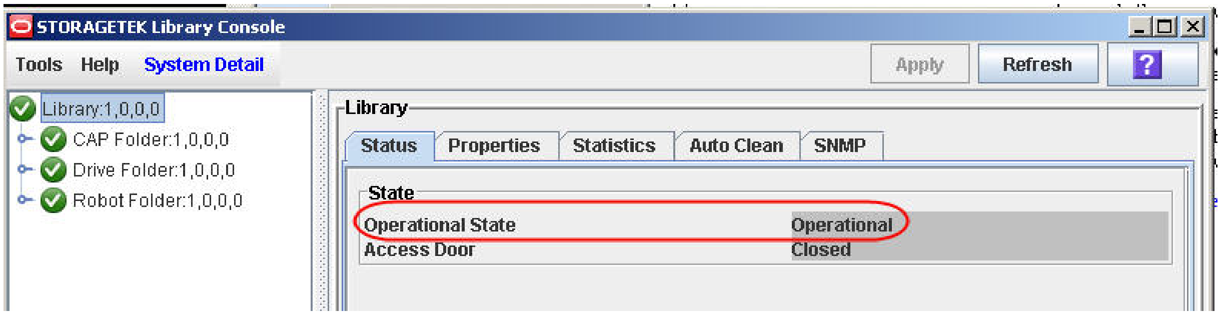
- "Test the SNMP Connection to the Library" on page 89
- "Get the Latest Configuration Data From the Library" on page 91

If the library is not fully initialized, then these procedures can be initiated but will likely fail because of the current library state.

> **Note –** For SL500, SL3000, and SL8500 libraries, you perform this procedure from a PC or workstation on which either the Standalone SL Console or the Web-based SL Console has been installed. For SL150 libraries, you use the browser-based user interface. See "Log In to the Library" on page 30 for details.

## ▼ SL500 Libraries

1. **Log in to the library with the SL Console.**
2. **Select System Detail > Library > Status.**
3. **Verify that the library state indicates "Operational".**

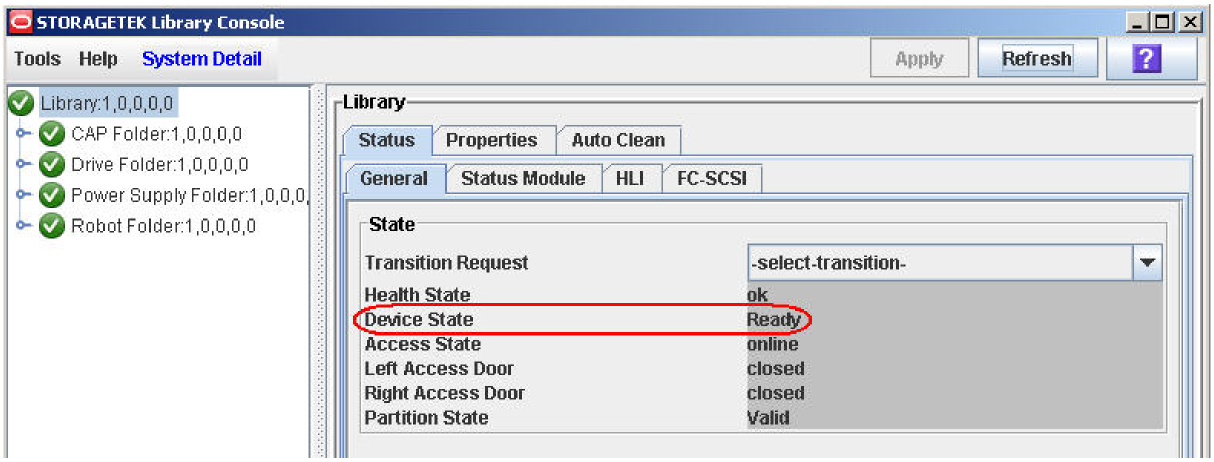


| | |
|---|---|
| Operational State | Operational |
| Access Door | Closed |

4. **Proceed to "Test the SNMP Connection to the Library" on page 89.**

## ▼ SL3000 and SL8500 Libraries

1. **Log in to the library with the SL Console.**
2. **Select System Detail > Library > Status > General.**
3. **Verify that the Device State indicates "Ready".**



State

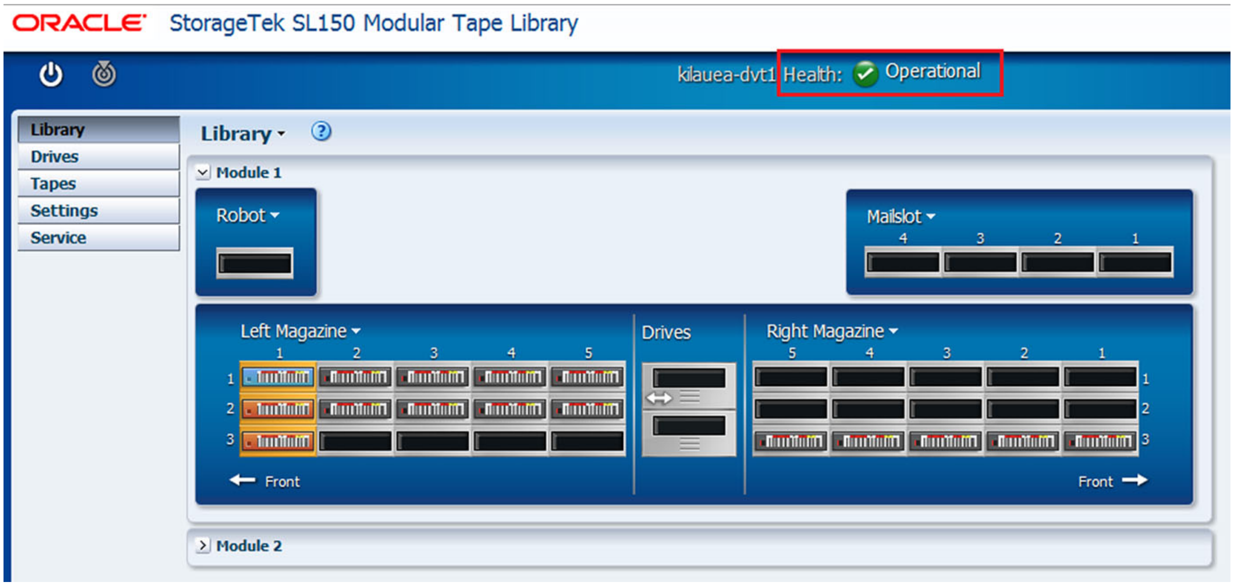
| | |
|---|---|
| Transition Request | -select-transition- |
| Health State | ok |
| Device State | Ready |
| Access State | online |
| Left Access Door | closed |
| Right Access Door | closed |
| Partition State | Valid |

4. Proceed to "Test the SNMP Connection to the Library" on page 89.

## ▼ SL150 Libraries

1. Log in to the browser-based user interface.

2. Verify that Health indicates "Operational".



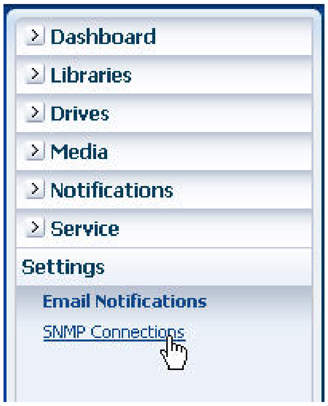
kilauea-dvt1 Health: Operational

## ▼ Test the SNMP Connection to the Library

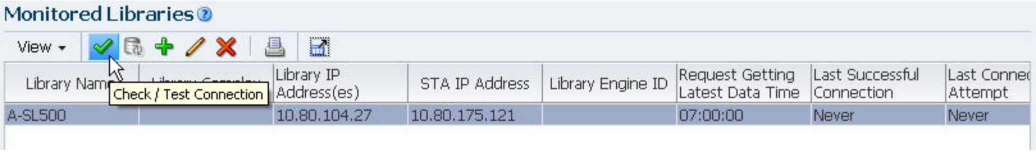
Use this procedure to test the SNMP connection between STA and a selected library. You should use this procedure whenever you add or modify SNMP connection information for either STA or the library. Only one library connection can be tested at a time. This process typically takes just seconds.

> **Note –** Before performing this procedure, you must verify that the library is fully initialized. See "Verify the Library is Operational" on page 87 for instructions.

1. **In the STA Navigation Bar, select Settings > SNMP Connections.**



2. **In the Monitored Libraries table, select the library you want to test. Click Check/Test Connection.**

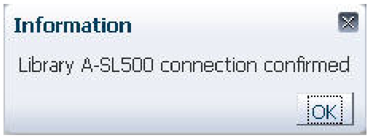


| Library Nam |  | Library IP Address(es) | STA IP Address | Library Engine ID | Request Getting Latest Data Time | Last Successful Connection | Last Connec Attempt |
|---|---|---|---|---|---|---|---|
| A-SL500 |  | 10.80.104.27 | 10.80.175.121 |  | 07:00:00 | Never | Never |

The test is initiated immediately.

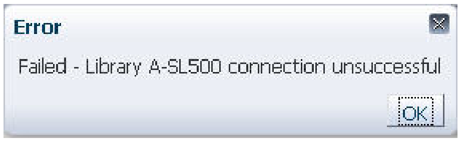
- If the test is successful, an information message appears.

  Click **OK** to dismiss the message and proceed to Step 3.



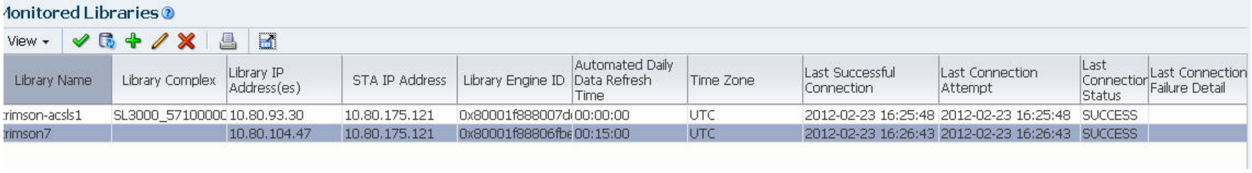
Library A-SL500 connection confirmed

- If the test is not successful, an error message appears. Click **OK** to dismiss the message. See "Troubleshoot an Unsuccessful SNMP Connection" on page 93 for suggestions.



Failed - Library A-SL500 connection unsuccessful

3. **Note the following updates in the Monitored Libraries table.**



| Library Name | Library Complex | Library IP Address(es) | STA IP Address | Library Engine ID | Automated Daily Data Refresh Time | Time Zone | Last Successful Connection | Last Connection Attempt | Last Connection Status | Last Connection Failure Detail |
|---|---|---|---|---|---|---|---|---|---|---|
| rimson-acsls1 | SL3000_5710000C | 10.80.93.30 | 10.80.175.121 | 0x80001f888007d | 00:00:00 | UTC | 2012-02-23 16:25:48 | 2012-02-23 16:25:48 | SUCCESS | |
| rimson7 | | 10.80.104.47 | 10.80.175.121 | 0x80001f88806fbe | 00:15:00 | UTC | 2012-02-23 16:26:43 | 2012-02-23 16:26:43 | SUCCESS | |

- The “Library Engine ID” field indicates the unique SNMP engine ID of the library.

  **Note –** A mismatch between the library engine ID shown here and the library engine ID specified when creating a trap recipient on the library does *not* affect the connection test.

- The “Last Successful Connection” and “Last Connection Attempt” fields indicate the date and time when the connection test was completed and initiated, respectively.

- The “Last Connection Status” field indicates “SUCCESS”.

- The “Library Complex” field is still blank; it will be updated after you get the latest configuration data from the library.

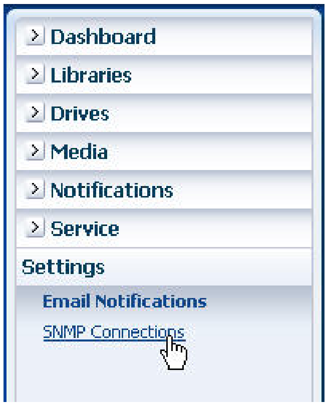
4. **Proceed to “Get the Latest Configuration Data From the Library” on page 91.**

## ▼ Get the Latest Configuration Data From the Library

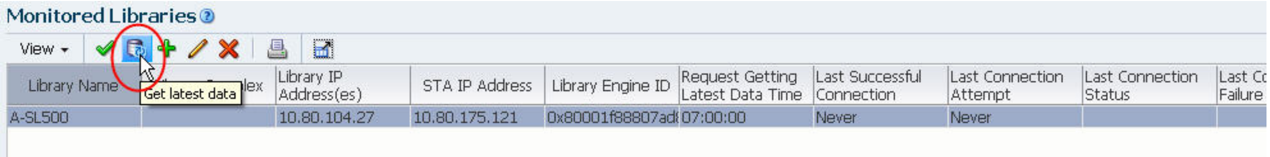
Use this procedure to manually initiate the configuration data collection process for a selected library. This process is performed automatically every 24 hours at the scheduled time of day, but this procedure allows you to initiate the process manually whenever you need to. You should use this procedure whenever you add SNMP connection information for a library. Only one data collection can be performed at a time.

> **Note –** Before performing this procedure, you must verify that the library is fully initialized. See "Verify the Library is Operational" on page 87 for instructions.

1. **In the STA Navigation Bar, select Settings > SNMP Connections.**

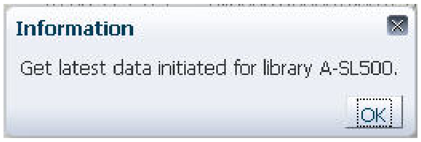


2. **In the Monitored Libraries table, select the library from which you want to collect configuration data, and click Get latest data.**



| Library Name | lex | Library IP Address(es) | STA IP Address | Library Engine ID | Request Getting Latest Data Time | Last Successful Connection | Last Connection Attempt | Last Connection Status | Last Co Failure |
|---|---|---|---|---|---|---|---|---|---|
| A-SL500 | | 10.80.104.27 | 10.80.175.121 | 0x80001f88807ad | 07:00:00 | Never | Never | | |

The data collection is initiated and an information message is displayed.



Information

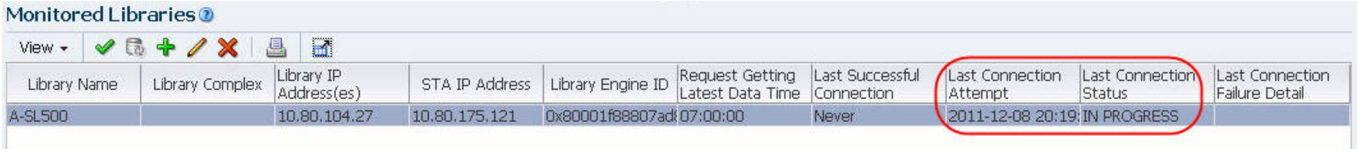
Get latest data initiated for library A-SL500.

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

Depending on the size of the library, the data collection process may take several minutes to an hour. The Last Connection Status in the Monitored Libraries table is updated, as follows:

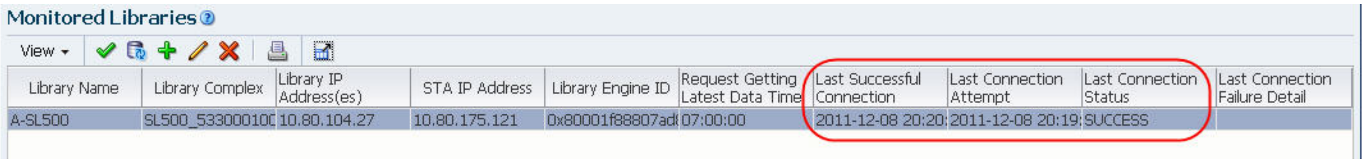
- While the process is underway, the Last Connection Status in the Monitored Libraries table indicates "IN PROGRESS" on the next screen refresh.

> **Note –** The default screen refresh interval is 480 seconds. If the Get latest data process completes before the next screen refresh, "IN PROGRESS" will not be displayed.



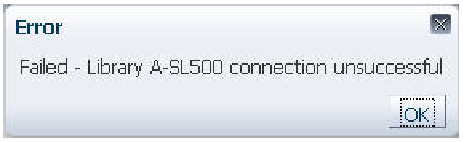
| Library Name | Library Complex | Library IP Address(es) | STA IP Address | Library Engine ID | Request Getting Latest Data Time | Last Successful Connection | Last Connection Attempt | Last Connection Status | Last Connection Failure Detail |
|---|---|---|---|---|---|---|---|---|---|
| A-SL500 | | 10.80.104.27 | 10.80.175.121 | 0x80001f88807ad | 07:00:00 | Never | 2011-12-08 20:19: | IN PROGRESS | |

- Once the process completes successfully, the status indicates “SUCCESS” and STA starts receiving exchange data from the library. Go to Step 4, below.



| Library Name | Library Complex | Library IP Address(es) | STA IP Address | Library Engine ID | Request Getting Latest Data Time | Last Successful Connection | Last Connection Attempt | Last Connection Status | Last Connection Failure Detail |
|---|---|---|---|---|---|---|---|---|---|
| A-SL500 | SL500_53300010C | 10.80.104.27 | 10.80.175.121 | 0x80001f88807ad | 07:00:00 | 2011-12-08 20:20: | 2011-12-08 20:19: | SUCCESS | |

- If the process was not successful, an error message is displayed. Click **OK** to dismiss the message.


Error

Failed - Library A-SL500 connection unsuccessful

If STA is able to provide information about why the data collection failed, it is displayed in the Last Connection Failure Detail field. See “Troubleshoot an Unsuccessful SNMP Connection” on page 93 for suggestions for resolving the issue.

> **Note –** The value displayed for Last Connection Failure Detail may extend beyond the width of the column. Be sure to extend the column width to see the entire value displayed.

4. **You have completed the SNMP configuration for STA. Proceed to** Chapter 3, “Configuring Email Notifications” on page 99**.**

# Configuration Troubleshooting

Use this section to troubleshoot connections between the server on which STA is installed and the library.

- "Troubleshoot an Unsuccessful SNMP Connection" on page 93
- "Troubleshoot Unsuccessful Trap Processing" on page 96

## ▼ Troubleshoot an Unsuccessful SNMP Connection

Use the procedures below to troubleshoot an unsuccessful library SNMP connection test or data collection. The order you choose to perform these procedures is at your discretion. You can use the "STA / Library Configuration Parameters Worksheet" on page 27 to help verify the correct configuration settings.

- What to Check on the Library
- What to Check on the Server

### ▼ What to Check on the Library

1. **Verify that the library is fully initialized. See "Verify the Library is Operational" on page 87.**

2. **Use the `traceroute` command to check communication from the server to the library.**

   a. **Log in to the server on which STA is installed.**

   b. **Issue the following command:**

   ```
   # traceroute -I library_IP_address_or_name
   ```

   Output will show the number of hops to the library, as well as the round-trip time to reach each hop. The round-trip time to the library (the last line in the command output) should be less than one second. If it is greater than one second, confirm the network's performance with your network administrator.

3. **Use the `traceroute` command to check communication from the library to the server.**

   a. **Log in to the library, as described in "Log In to the Library" on page 30.**

   b. **Issue the following command, depending on the library type:**

   - SL8500 and SL3000:

     ```
     traceRoute sta_server_IP_address
     ```

   - SL500:

     ```
     traceroute sta_server_IP_address
     ```

     **Note –** On SL500 libraries, the `traceroute` command is available with FRS 1468 and above.

Output will show the number of hops to the server, as well as the round-trip time to reach each hop. The round-trip time to the server (the last line in the command output) should be less than one second. If it is greater than one second, confirm the network's performance with your network administrator.

4. **Use the `snmp enable` command to ensure that SNMP has been enabled on the public port. See "Enable SNMP on the Library" on page 46.**

   **Note –** This is not applicable to SL150 libraries. On SL150 libraries, SNMP is enabled by default.

5. **Verify that there is one and only one SNMP v2c user, if applicable. (See "Ensure an SNMP v2c User" on page 49 to see if a v2c user is required in your case.)**

   - On SL500, SL3000, and SL8500 libraries, use the **`snmp listUsers`** command to view a list of SNMP users.
   - On SL150 libraries, go to Settings > SNMP > SNMP Users.

6. **Verify that the SNMP v3 user was added correctly. (See "Create an SNMP v3 User" on page 55 for details.)**

   - On SL500, SL3000, and SL8500 libraries, use the **`snmp listUsers`** command to view a list of SNMP users.
   - On SL150 libraries, go to Settings > SNMP > SNMP Users.

   **Note –** If you're using SNMP v2c, see appendix "Configuring SNMP v2c Mode" on page 197.

   **Note –** For SL500 libraries, verify the username or passwords do not contain single quotes as text.

   **Note –** To verify SNMP communications, see "Verify SNMP Communications With the Library" on page 76.

   **Name** – Must match the SNMP User Name on the STA SNMP Client Attributes screen, as well as the SNMP user specified when creating an SNMP trap recipient on the library.

   **Version** – Must be v3.

   **Auth** – Must be SHA.

   **Priv** – Must be DES.

   **Auth Pass** and **Priv Pass** – Must match the passwords on the STA SNMP Client Attributes screen, as well as the passwords specified when creating a trap recipient on the library.

7. **Use the `snmp engineId` (for SL500 libraries) or `snmp engineId print` (for SL3000 and SL8500 libraries) command to display the library engine ID.**

   **Note –** These commands are not applicable to SL150 libraries.

   The entry must not contain any upper-case characters. For the SL8500 and SL3000 libraries, the entry must include the 0x prefix (the SL500 may also show this prefix). See "Create an SNMP v3 User" on page 55.

8. **Verify that STA has been correctly configured as a trap recipient. (See "Create an SNMP v3 Trap Recipient" on page 61 for details).**

- On SL500, SL3000, and SL8500 libraries, use the **`snmp listTrapRecipients`** command to display a list of trap recipients on the library.
- On SL150 libraries, go to Settings > SNMP > SNMP Trap Recipients.

  **Note –** If you're using SNMP v2c, see appendix "Configuring SNMP v2c Mode" on page 197.

  **Note –** For SL500 libraries, verify the passwords do not contain single quotes as text.

**Engine Id** – Must match the library engine ID displayed in Step 7. The entry must not contain any upper-case characters. For the SL8500 and SL3000 libraries, the entry must include the 0x prefix (the SL500 may also show this prefix). See "Create an SNMP v3 User" on page 55.

> **Note –** Checking the engine ID is not applicable to SL150 libraries, as the engine ID is automatically obtained.

**Host** – IP address of the STA server.

**Version** – Must be v3.

**Auth** – Must be SHA.

**Priv** – Must be DES.

**Auth Pass** and **Priv Pass** – Must match the passwords on the STA SNMP Client Attributes screen, as well as the passwords specified when creating an SNMP user.

9. **For SL500 libraries, use the `staConfig` command to verify that "STA mode" has been enabled. See "Set the SL500 Volume Label Format" on page 68.**
10. **For SL150 libraries, go to Settings > Library to ensure Volume Label Format is set to "Trim last two characters". See "Set the SL150 Volume Label Format" on page 70.**
11. **If you find any data entry errors, use the appropriate commands to fix them, and then try the SNMP connection procedure again.**
12. **As a last resort, after checking all other options on both the library and STA, consider deleting and re-adding the SNMP v3 user.**

## ▼ What to Check on the Server

1. **Ensure the server on which STA is installed is using a static IP address.**

   The server cannot use a dynamically-assigned (DHCP) address.

2. **Verify that the library public port is reachable from the STA server by pinging the primary IP address and, if applicable, the secondary IP address.**
3. **Display the STA SNMP Client Attributes screen, and verify that the settings exactly match the corresponding settings for the SNMP v3 user and SNMP v3 trap recipient on the library. See "Configure SNMP Client Settings for STA" on page 80.**

   - **SNMP Connection User Name** – User name you created for the SNMP v3 user and trap recipient on the library.
   - **SNMP Connection Password** – Connection authorization password for the SNMP v3 user and trap recipient on the library.

- **Privacy Encryption Password** – Privacy encryption password for the SNMP v3 user and trap recipient on the library.

4. **Display the STA Monitored Libraries screen, and verify that the settings exactly match the corresponding settings for the SNMP v3 user on the library. See "Configure SNMP Connections With the Library" on page 84.**

   - **Library Primary IP Address** – IP address of the primary public port on the library. See "Retrieve the Library IP Address" on page 36 for the correct entry.
   - **Library Secondary IP Address** – IP address of the secondary public port on the library, if applicable. For SL500 and SL150 libraries, this field is always blank. For SL3000 and SL8500 libraries, see "Retrieve SL3000 or SL8500 IP Addresses" on page 36 for the correct entry.
   - **STA IP Address** – IP address of the STA server.
   - **Library Engine ID** – SNMP engine ID of the library. The entry must not contain any upper-case characters. For the SL8500 and SL3000 libraries, the entry must include the 0x prefix (the SL500 library may also show this prefix).

     **Note –** Checking the engine ID is not applicable to SL150 libraries, as the engine ID is automatically obtained.

     **Note –** When initially entering library details in the STA GUI, leave the Library Engine ID blank. It will be filled in by STA after you select the library and perform a "Test Connection".

5. **If you find any data entry errors, fix them on the appropriate screen, and then try the SNMP connection procedure again.**

# ▼ Troubleshoot Unsuccessful Trap Processing

If traps are not being received by the STA host, or traps are not being processed by STA, perform the following.

1. **Ensure the server on which STA is installed is using a static IP address.**

   The server cannot use a dynamically-assigned (DHCP) address.

2. **Within a separate terminal window, enter the following command:**

   ```
   # tcpdump -v host library-public-port
   ```

   - *library-public-port* is the IP address of the primary public port on the library. See "Retrieve the Library IP Address" on page 36 for the correct entry.
   - In the output, look for ".snmptrap" and "SNMPv3". Network traffic that meets "Get Latest Data" requests will be ".snmp".
   - If there is activity on the library, but no traps are being received, then check the library trap recipient entry for accuracy. See "Troubleshoot an Unsuccessful SNMP Connection" on page 93.

3. **Ensure SNMP port 162 is available for STA.**

   The STA trap listener processes traps through port 162. To troubleshoot communications over this port, do the following.

a. **Check the `/Oracle/Middleware/user_projects/domains/TBI/servers/staServer/logs/staServer.log` file for a "SEVERE" error, such as:**

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

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

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

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

```
# chkconfig --list
```

4. **If snmpd or snmtrapd are running, then ensure that they are turned off permanently.**

   a. **Deconfigure SNMP services:**

```
# chkconfig snmpd off
# chkconfig snmptrapd off
```

   b. **Stop SNMP services:**

```
# service snmptrapd stop
# service snmpd stop
```

   c. **Stop and restart STA services:**

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

5. **If some traps are being reported in the Notifications screen, ensure that ALL trap levels were specified when creating a trap recipient on the library. See "Create an SNMP v3 Trap Recipient" on page 61 for the list of supported trap levels.**

6. **For the SL500, ensure you configured the library with a supported version of SL Console. Earlier versions of SL Console restricted the number of trap level characters that could be entered. See "Library Software Requirements" in the** *STA Planning and Installation Guide* **for the minimum supported SL Console version.**

3

# Configuring Email Notifications

STA sends email notifications when it detects significant events. These events may be a direct result of something that happens in the tape environment, such as an error report by a tape library.

Notifications include these elements:

- A message type, which gives a method for grouping for notifications. Similar messages, for example drive messages, have the same message type.
- A reference to some entity in the model or warehouse tables, such as a drive, media, or library.
- Date and time the notification was created.

This chapter includes the following topics:

- "How Email Notifications Work" on page 100
- "Message Types" on page 101
- "Email Tasks" on page 102

# How Email Notifications Work

STA sends email notifications when the hardware status of the four monitored device-types changes state, either moving to a better state or to a worse state.

All devices have the same states:

- NORMAL (good)
- DEGRADED
- NOTOPERATIVE (bad)
- UNKNOWN (no previous traps from the device)

Devices follow the identical rules to decide when to generate an email.

TABLE 3-1 shows the triggers that cause an email notification.

**TABLE 3-1** Notification Causes

| Hardware Impacted | Condition/Status Change |
|---|---|
| Library top-level, Drive, PTP, and CAP | • NORMAL to DEGRADED<br>• NORMAL to NOTOPERATIVE<br>• DEGRADED to NOTOPERATIVE<br>• UNKNOWN to DEGRADED<br>• UNKNOWN to NOTOPERATIVE<br>• NOTOPERATIVE to DEGRADED<br>• NOTOPERATIVE to NORMAL<br>• DEGRADED to NORMAL<br>• UNKNOWN to NORMAL |

# Message Types

When STA detects an event, it creates a record in the database and sends a message in an email notification.

The following types of messages are sent by STA.

- Test Message
- Drive Message
- CAP Message
- PTP Message
- Library Message

## Test Message

STA sends a test message to confirm an email address when email notifications are established or modified. An example is:

```
October 11, 2011 9:24:56 AM MDT === Alert Test Message from STA
Server at 127.0.0.1
```

## Drive Message

A drive message notes a drive condition change. An example is:

```
October 5, 2011 6:44:50 AM MDT === Drive Condition Change: The
condition of HpUltrium3 (SN: HU1044939C, LOCATION: 1.4.-2.1.1) has
changed from notoperative to degraded.
```

## CAP Message

A CAP message signals a CAP condition change. An example is:

```
October 5, 2011 10:52:57 PM MDT === CAP Condition Change: The
condition of 1.2.39.2.0 in SL8500 elib7 (SN: 516000201043) has
changed from unknown to degraded.
```

## PTP Message

A PTP message shows a PTP condition change. An example is:

```
October 5, 2011 1:56:46 AM MDT === PTP Condition Change: The
condition of 0,1,2,3 in SL8500 Library 1 (SN: 1853854938) has
changed from normal to notoperative.
```

## Library Message

A library message that details a library condition change. An example is:

```
October 5, 2011 10:53:25 PM MDT === Library Condition Change: The
condition of SL8500 elib7 (SN: 516000201043) has changed from
DEGRADED to NOTOPERATIVE.
```

# Email Tasks

To configure email notifications, do the following:

- "Define SMTP Server Details" on page 102.
- "Add an Email Address" on page 105.
- "Test your SMTP and Email Address Setup" on page 106.

To modify or delete an email address, do the following:

- "Edit an Email Address" on page 106.
- "Delete an Email Address" on page 107.

## ▼ Define SMTP Server Details

1. **Point your browser to the STA GUI login screen.**

   http://*yourHostName*:7021/STA/

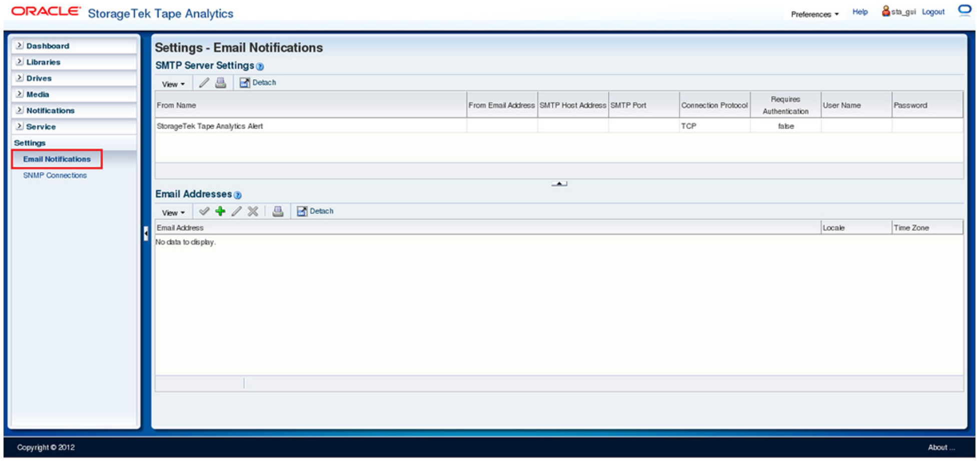
   or

   https://*yourHostName*:7022/STA/

   > **Note –** Use the HTTP or HTTPS port number you selected during STA installation.

2. **Log in using the STA GUI Login username and password you defined during STA installation.**

3. **From the STA accordion, click Settings -> Email Notifications.**



Settings - Email Notifications

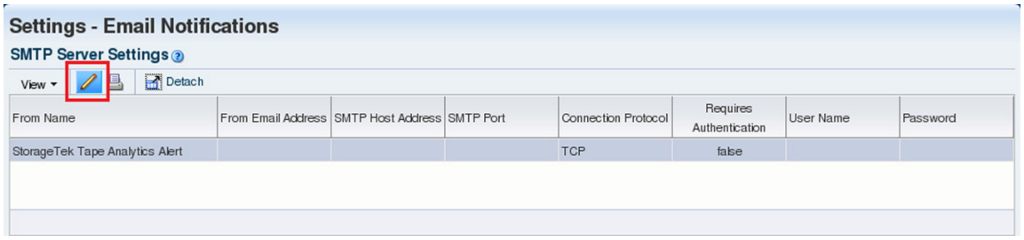
SMTP Server Settings

| From Name | From Email Address | SMTP Host Address | SMTP Port | Connection Protocol | Requires Authentication | User Name | Password |
|---|---|---|---|---|---|---|---|
| StorageTek Tape Analytics Alert | | | | TCP | false | | |

Email Addresses

| Email Address | Locale | Time Zone |
|---|---|---|
| No data to display. | | |

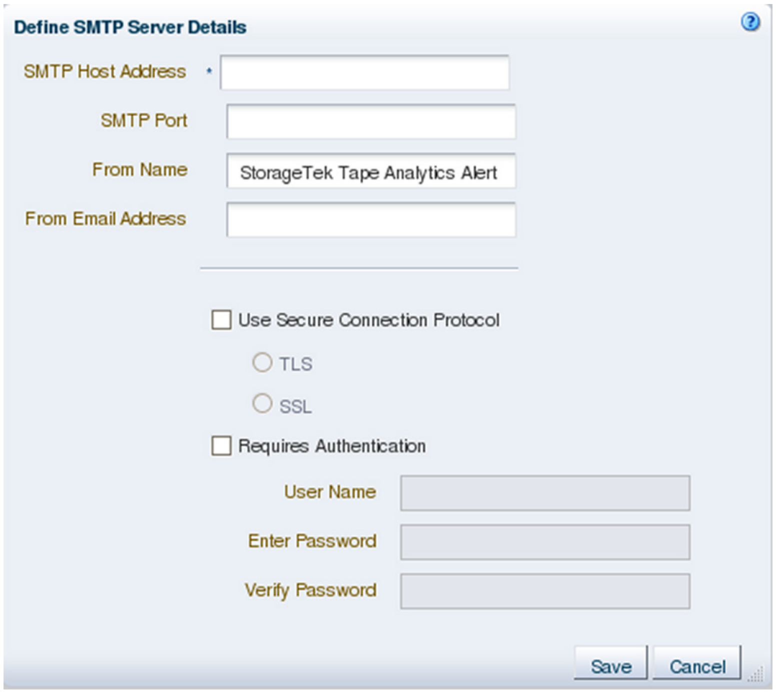
4. **In the SMTP Server Settings table, select StorageTek Tape Analytics Alert, then click the Edit Selected SMTP Server icon located in the toolbar.**



| From Name | From Email Address | SMTP Host Address | SMTP Port | Connection Protocol | Requires Authentication | User Name | Password |
|---|---|---|---|---|---|---|---|
| StorageTek Tape Analytics Alert | | | | TCP | false | | |

5. **In the Define SMTP Server Details window, enter the IP address of your SMTP email server.**

   > **Note –** If the email server does not require authentication, you may need to specify `localhost` for the SMTP Host Address.



| | |
|---|---|
| SMTP Host Address * | |
| SMTP Port | |
| From Name | StorageTek Tape Analytics Alert |
| From Email Address | |

☐ Use Secure Connection Protocol

○ TLS

○ SSL

☐ Requires Authentication

| | |
|---|---|
| User Name | |
| Enter Password | |
| Verify Password | |

6. **Enter the SMTP port number for outgoing mail transport.**

   Typically, this is port 25, but check with your IT administrator to verify that this is the port used at your site (sites can use other ports for SMTP).

7. **Enter the name you want the From line in your email to display.**

   Text that identifies the server on which STA is installed is recommended, so you know the source of the message when it arrives in your email.

8. **Enter the email address from which the email is being sent.**

   Since you cannot reply to this address (the server does not receive emails), you may want to enter an address that indicates this. For example:

   `DoNotReply@YourCompany.com`

9. **Select the Use Secure Connection Protocol check box to select the appropriate secure connection protocol (TLS or SSL).**

See your IT administrator to determine which connection is right for you.

10. **Select the Requires Authentication check box if the SMTP server requires authentication.**

    a. **Enter a user name supported by the SMTP server.**

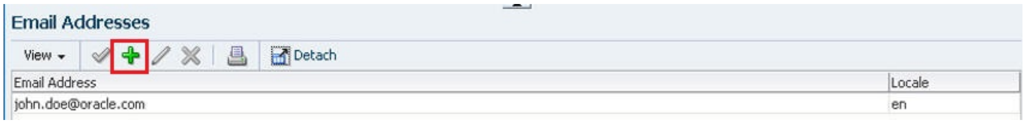
    b. **Enter and verify the correct password for that email user.**

11. **Click Save.**

## ▼ Add an Email Address

Email notifications are sent to all configured email destinations. To add an email address, do the following.

1. **Click the Add Email icon located in the toolbar.**



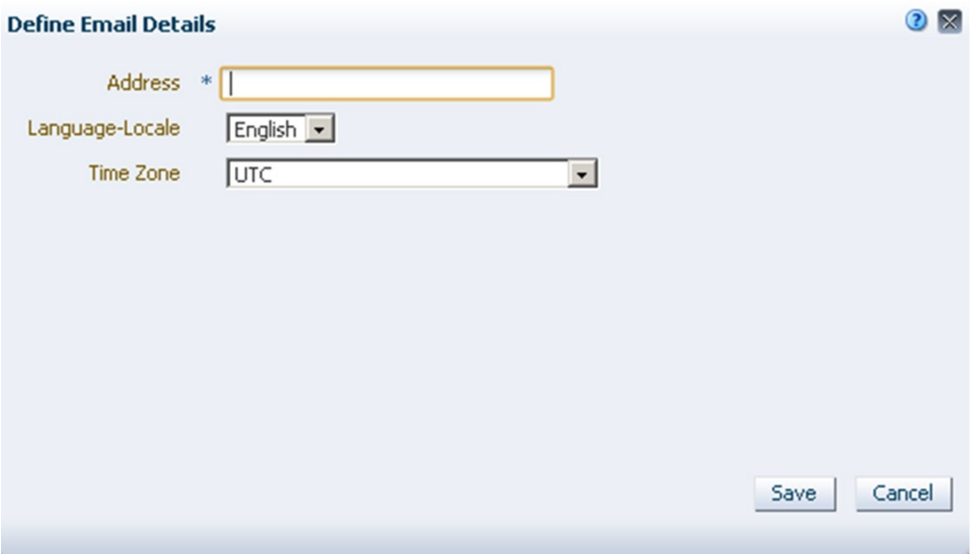
Email Addresses

| Email Address | Locale |
|---|---|
| john.doe@oracle.com | en |

2. **In the Define Email Details dialog box, enter a destination for email notifications.**

   For example:

   `yourname@your.company.com`



Define Email Details

Address *

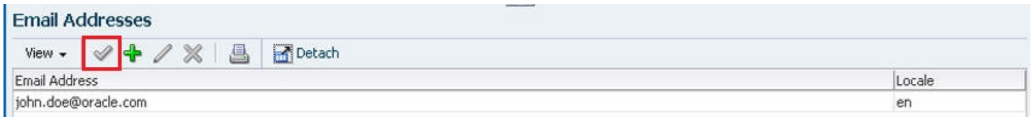
Language-Locale: English

Time Zone: UTC

3. **In the Language-Locale list, select the desired language-locale.**
4. **In the Time Zone list, select the recipient's time zone.**
5. **Click Save.**

## ▼ Test your SMTP and Email Address Setup

1. **To test your setup, click the Test SMTP and email address setup icon located in the toolbar and email address setup.**



| Email Address | Locale |
|---|---|
| john.doe@oracle.com | en |

2. **Go to your email client where you expect to receive the email.**

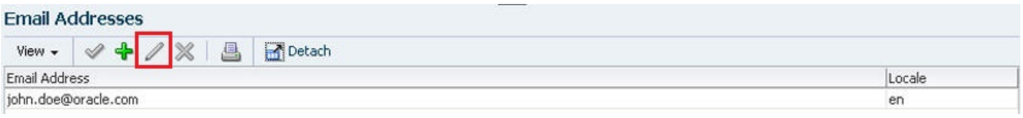
   The test email should arrive momentarily, depending on your email system and servers. If the test email does not arrive, check your STA configuration. If your configuration looks good, check with your system email administrator.

   > **Note –** You can view the following log file to check for email configuration problems:
   >
   > **`/Oracle/Middleware/user_projects/domains/TBI/servers/staServer/logs/staServer.log`**

## ▼ Edit an Email Address

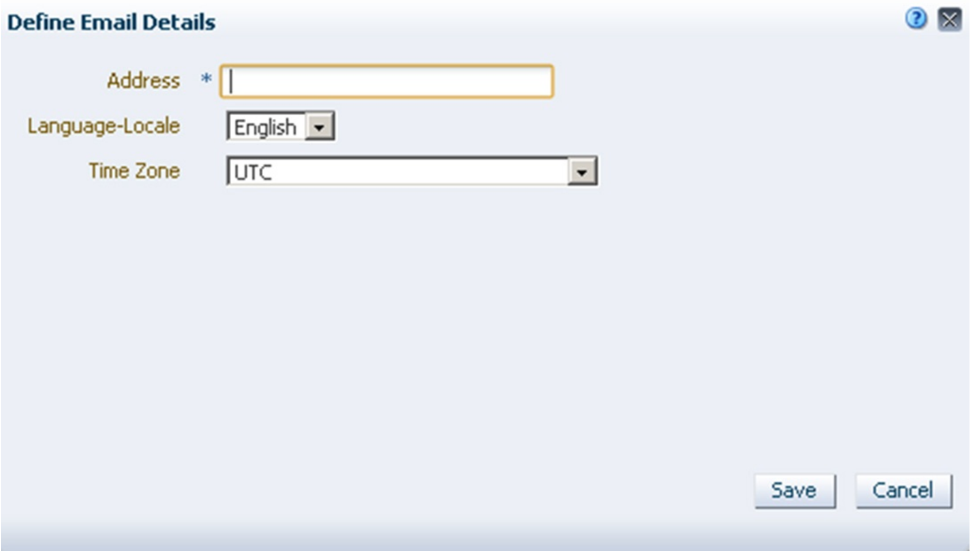
To edit an email address, do the following:

1. **Select an email address from the table, then click the Edit Selected Email icon.**



| Email Address | Locale |
|---|---|
| john.doe@oracle.com | en |

2. **In the Define Email Details dialog box, make any necessary changes to the email address you selected.**



Define Email Details

Address *

Language-Locale: English

Time Zone: UTC

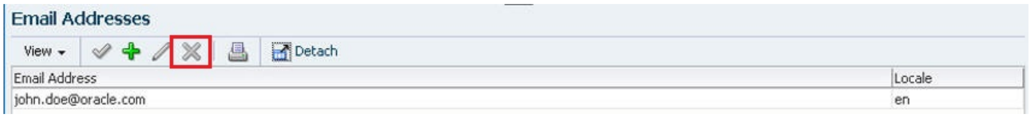
3. **Click Save.**

## ▼ Delete an Email Address

To delete an email address, do the following.

1. **Select the email addresses you want to delete.**
2. **Click the Delete Selected Email(s) icon located in the toolbar.**

   The selected emails are deleted.



Email Addresses

| Email Address | Locale |
|---|---|
| john.doe@oracle.com | en |

# 4

# Configuring STA Services

You will use the following process after initial installation of the STA application to configure the STA Backup and STA Resource Monitor services so they begin performing their functions. Then you can use selected procedures as needed to modify the settings for the services.

**Preparation Task**

1. "Optional: Update Linux PATH Setting" on page 110.

**Backup Configuration Tasks**

2. "Review the staservadm Utility Preferences" on page 111.
3. "Determine STA Backup Preferences" on page 112.
4. "Configure the Remote Backup Server" on page 113.
5. "Configure the STA Backup Service" on page 114.

**Resource Monitor Configuration Tasks**

6. "Review the staresmonadm Utility Preferences" on page 117.
7. "Determine STA Resource Monitor Preferences" on page 119.
8. "Configure the STA Resource Monitor" on page 120.

**Services Daemon Task**

9. "Restart the STA Services Daemon (optional)" on page 123.

# Preparation Task

## ▼ Optional: Update Linux PATH Setting

You can use this procedure to update the Linux PATH environment variable to include the location of the STA service utilities (**`staservadm`** and **`staresmonadm`**). By default, the location is the following directory:

```
/Oracle/StorageTek_Tape_Analytics/common/bin
```

1. **Open the profile for your user ID with a text editor.**

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

2. **Add the above directory to the PATH definition.**

   For example:

```
# .bash_profile

# User specific environment and startup programs

PATH=$PATH:$HOME/bin
PATH=$PATH:/Oracle/StorageTek_Tape_Analytics/common/bin

export PATH
```

3. **Save and exit the file.**
4. **Log out and log back in to Linux.**
5. **Display the setting for the PATH environment variable. The above STA directory should be displayed.**

   For example:

```
# echo $PATH
/usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/sbin:/usr/
local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin:/Oracle/
StorageTek_Tape_Analytics/common/bin
```

6. **Proceed to** "Backup Configuration Tasks" on page 111**.**

# Backup Configuration Tasks

## ▼ Review the staservadm Utility Preferences

You configure the STA Backup service with the STA Backup Service Administration Utility, staservadm. Review TABLE 4-1 for descriptions of the available preference settings to use in the next procedure, "Determine STA Backup Preferences" on page 112.

> **Note –** To display a complete list of command options, type "**`staservadm -h`**" at the command line. To see the current Backup Services settings, type "**`staservadm -Q`**" at the command line.

**TABLE 4-1** staservadm Attributes

| Attribute | Option | Description | Default Value |
|---|---|---|---|
| Backup host name | **`-s`** | IPv4 or IPv6 address, or fully qualified DNS host name, of the server host to which the STA server copies its backup files. | N/A |
| Backup user ID | **`-u`** | System user ID of the user authorized to perform SCP file transfers to the backup host. | N/A |
| Backup password | **`-p`** | Password assigned to the backup user. | N/A |
| Backup directory | **`-d`** | Directory on the backup host where the backup files will be copied. | N/A |
| Database username | **`-U`** | Database username authorized to perform a **`mysqldump`** command.<br>You should specify the **`stadba`** (STA Database Administrator) username that was created when the STA application was installed. For details, see the "Installing STA" chapter within the *StorageTek Tape Analytics Planning and Installation Guide*. | N/A |
| Database password | **`-P`** | Password of the database user.<br>This must be the password assigned to the database username when the STA application was installed. For details, see the "Installing STA" chapter within the *StorageTek Tape Analytics Planning and Installation Guide*. | N/A |

**TABLE 4-1** staservadm Attributes (Continued)

| Attribute | Option | Description | Default Value |
|---|---|---|---|
| File transfer type | **-F**\|**-S** | Method of file transfer used to copy the backup files from the STA server to the backup host. Options are SCP (**-S**) or FTP (**-F**). Oracle recommends SCP. | **-S** (SCP) |
| Full backup dump time | **-T** | Time of day when you want a full database backup dump to be performed. The dump is performed automatically every 24 hours at approximately this time. The actual time is sometime within "sleep interval" seconds after this time.<br>Format is **hh:mm**, using 24-hour time (for example, 13:15 is 1:15 pm). | 00:00 |
| Sleep interval | **-i** | Number of seconds the STA Services daemon waits before checking for new incremental backup files. | 300 |

## ▼ Determine STA Backup Preferences

Use this procedure to determine the attribute settings you want to use for the STA Backup service.

> **Note –** Oracle recommends that you configure a remote backup server to receive the backup files.

1. **See TABLE 4-1 on page 111 for descriptions of the available attributes.**
2. **Complete the STA Backup Service Worksheet (TABLE 4-2) for your site.**

**TABLE 4-2** STA Backup Service Worksheet

| Attribute | Option | My Setting | Default |
|---|---|---|---|
| Backup host name | **-s** | | N/A |
| Backup user ID | **-u** | | N/A |
| Backup password | **-p** | | N/A |
| Backup directory | **-d** | | N/A |
| Database username | **-U** | | N/A |
| Database password | **-P** | | N/A |
| File transfer type | **-F**\|**-S** | | **-S** (SCP) |
| Full dump time | **-T** | | 00:00 |
| Sleep interval | **-i** | | 300 |

3. **Proceed to "Configure the Remote Backup Server" on page 113.**

## ▼ Configure the Remote Backup Server

Use this procedure to configure a remote server to receive the backup files generated by the STA Backup service.

> **Note –** You perform this procedure on the backup server.

1. **On the backup server, log in as the system root user.**
2. **Create a new group for the STA Backup user.**

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

In this example, the group ID is “stabckgr”, and the following option is used:

- `-g` – Assign the specified numerical GID to the group.

3. **Create the STA Backup user.**

```
# 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` – Full 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.**

> **Note –** Be sure to make a record of the user ID and password.

```
# 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.**

```
# 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. The following option is used.

- **-p** – Make parent directories as needed.

6. **Display the user attributes to confirm that all information has been entered correctly.**

```
# 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.**

```
# chown -R stabck:stabckgr STAbackups
# chmod -R 600 STAbackups
#
```

In this example, the following option is used:

- **-R** – Recursively assign the attributes to the directory and its files.

8. **List the directory to confirm that all information has been entered correctly.**

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

9. **Proceed to “Configure the STA Backup Service” on page 114.**

## ▼ Configure the STA Backup Service

Use this procedure to configure the STA 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 one of the following occurs:

- The STA Backup service wakes up from its current sleep interval and processes the new settings.
- You manually restart the STA Services daemon. See “Restart the STA Services Daemon (optional)” on page 123 for instructions.

1. **On the STA server, log in as the system root user.**
2. **Display the current STA Backup Service settings.**

   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      -X [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 []
 =======================================
```

3. **With the STA Backup Service Worksheet as a reference, use the staservadm command to set the attribute values to the settings you want.**

   **Note –** You can submit the attributes in separate commands, or you can combine them all into one. The following example shows all attributes submitted in one command.

```
# staservadm -s sta.backups.com \
> -u stabck -p bckpwd1 \
> -d /home/stabck/STAbackups \
> -U stadba -P dbapwd1 \
> -T 02:00
> -S -i 600
```

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

```
Contacting daemon...connected.
Setting File Transfer Type... SCP
Setting Sleep Interval....... 600
Setting Backup Hostname...... sta.backups.com
Setting Backup Username...... stabck
Setting Backup Password...... *******
Setting Backup Directory..... /home/stabck/STAbackups
Setting Database Username.... stadba
Setting Database Password.... *******
Done.
 Current STA Backup Service Settings:
   File Transfer        -S [SCP]
   Full Backup          -T [02:00]
   Sleep Interval       -i [600 sec]
   Backup Hostname      -s [sta.backups.com]
   Backup Username      -u [stabck]
   Backup Password      -p [*******]
   Backup Directory     -d [/home/stabck/STAbackups]
   Database Username    -U [stadba]
   Database Password    -P [*******]
 =======================================
#
```

4. **Review the command output to verify that the values have been set correctly. If you need to make corrections, you can resubmit just the attributes that need to be changed.**

```
# staservadm -i 300
Contacting daemon...connected.
Setting Sleep Interval....... 300
Done.
 Current STA Backup Service Settings:
   File Transfer        -S [SCP]
   Full Backup          -T [02:00]
   Sleep Interval       -i [300 sec]
   Backup Hostname      -s [sta.backups.com]
   Backup Username      -u [stabck]
   Backup Password      -p [*******]
   Backup Directory     -d [/home/stabck/STAbackups]
   Database Username    -U [stadba]
   Database Password    -P [*******]
 =======================================
#
```

5. **Proceed to "Determine STA Resource Monitor Preferences" on page 119.**

# Resource Monitor Configuration Tasks

## ▼ Review the staresmonadm Utility Preferences

You configure the STA Resource Monitor service with the STA Resource Monitor Administration Utility, staresmonadm. Review TABLE 4-3 for descriptions of the available preference settings to use in the next procedure, "Determine STA Resource Monitor Preferences" on page 119.

**Note –** To display a complete list of command options, type "**`staresmonadm -h`**" at the Linux command line.

**TABLE 4-3** staresmonadm Attributes

| Attribute | Option | Description | Default Value |
|---|---|---|---|
| Database tablespace HWM | **`-t`** | High-water mark for the database tablespace. Entered as a percentage of the maximum available; for example, 80 indicates 80%. | -1 (indicates the attribute has not been configured) |
| Database disk volume HWM | **`-d`** | High-water mark for the disk volume on which the database data files reside, usually **`/dbdata/mysql`**. Entered as a percentage of the maximum available; for example, 80 indicates 80%. | -1 (indicates the attribute has not been configured) |
| Logging disk volume HWM | **`-l`** | High-water mark for the disk volume on which the STA logs are located, usually **`/var/log/tbi`**. Entered as a percentage of the maximum available; for example, 80 indicates 80%. | -1 (indicates the attribute has not been configured) |
| Physical memory (RAM) HWM | **`-m`** | High-water mark for the total installed physical system memory. Virtual memory is not taken into account. Entered as a percentage of the maximum available; for example, 80 indicates 80%. | -1 (indicates the attribute has not been configured) |
| Email from | **`-f`** | Name or email address you want to appear in the "From" field of the standard daily report email. | **`StaResMon@localhost`** |
| Email recipients | **`-r`** | Recipient email addresses, entered as a colon-delimited list. | N/A |
| Email subject | **`-s`** | Entry you want to appear in the "Subject" field of the standard daily report email. Enter up to 128 characters.<br>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 |

**TABLE 4-3** staresmonadm Attributes (Continued)

| Attribute | Option | Description | Default Value |
|---|---|---|---|
| Database username | **`-U`** | Database username authorized to perform queries against the "**`information_schema`**" database tables and the MySQL server internal system global variables.<br>You should specify either the **`stadba`** (STA Database Administrator) username or the MySQL **`root`** username that was created when the STA application was installed. For details, see the "Installing STA" chapter within the *StorageTek Tape Analytics Planning and Installation Guide*. | N/A |
| Database password | **`-P`** | Password of the database user.<br>This must be the password assigned to the database username when the STA application was installed. For details, see the "Installing STA" chapter within the *StorageTek Tape Analytics Planning and Installation Guide*. | N/A |
| Daily report send time | **`-T`** | Time of day when you want the standard daily report to be sent. The report is sent automatically every 24 hours at approximately this time. The actual time is sometime within "sleep interval" seconds after this time.<br>Format is **`hh:mm`**, using 24-hour time (for example, 13:15 is 1:15 pm). | 00:00 |
| Sleep interval | **`-i`** | Number of seconds the STA Resource Monitor waits between scans. | 600 |
| Output data file | **`-o`** | Full path of the output data file, which is a comma-separated file (.csv). | **`/var/log/tbi/db/staresmon.csv`** |
| "Nag" mode | **`-n`** | Indicates how frequently alerts are sent if any high-water marks have been breached.<br>• If set to "on", alert emails are sent every time the system is scanned.<br>• If set to "off", alerts are simply noted in the standard daily report. | off |
| Query | **`-Q`** | Display the current STA Resource Monitor service settings. | N/A |

## ▼ Determine STA Resource Monitor Preferences

Use this procedure to determine the attribute settings you want to use for the STA Resource Monitor service.

1. **See TABLE 4-3 on page 117 for descriptions of the available attributes.**
2. **Complete the STA Resource Monitor Attributes Worksheet (TABLE 4-4) for your site.**

**TABLE 4-4** STA Resource Monitor Attributes Worksheet

| Attribute | Option | My Setting | Default |
|---|---|---|---|
| Database tablespace HWM (percent) | `-t` | | -1 (indicates the attribute has not been configured) |
| Database disk volume HWM (percent) | `-d` | | -1 (indicates the attribute has not been configured) |
| Logging disk volume HWM (percent) | `-l` | | -1 (indicates the attribute has not been configured) |
| Physical memory (RAM) HWM (percent) | `-m` | | -1 (indicates the attribute has not been configured) |
| Email from (name or email ID) | `-f` | | `StaResMon@localhost` |
| Email recipients (colon-delimited list) | `-r` | | N/A |
| Email subject | `-s` | | STA Resource Monitor Report |
| Database username (MySQL root or stadba, created when the STA application was installed) | `-U` | | N/A |
| Database password (password assigned to the username) | `-P` | | N/A |
| Daily report send time (`hh:mm`) | `-T` | | 00:00 |
| Sleep interval (seconds) | `-i` | | 300 |
| Output data file | `-o` | | `/var/log/tbi/db/staresmon.csv` |
| Nag mode (on/off) | `-n` | | off |

3. **Proceed to "Configure the STA Resource Monitor" on page 120.**

## ▼ Configure the STA Resource Monitor

Use this procedure to configure the STA Resource Monitor service. Your configuration settings take effect as soon as one of the following occurs:

- The STA Resource Monitor service wakes up from its current sleep interval and processes the new settings.
- You manually restart the STA Services daemon. See "Restart the STA Services Daemon (optional)" on page 123 for instructions.

1. **On the STA server, log in as the system `root` user.**

2. **Display the current STA Resource Monitor settings.**

   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 [stadba]
   DB Password         -P [********]
   DB Tablespace hwm   -t [-1%]
   DB Disk Volume hwm  -d [-1%]
   STA Log Volume hwm  -l [-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. **With the STA Resource Monitor Worksheet as a reference, use the `staresmonadm` command to set the attribute values to the settings you want.**

   > **Note –** You can submit the attributes in separate commands, or you can combine them all into one. The following example shows all attributes submitted in one command.

```
# staresmonadm -t 65 -d 65 -l 65 -m 95 \
> -f STAMonitor@localhost \
> -r STAadmin@MyCompany.com:ABCadmin@MyCompany.com \
> -s ‘STA Resource Monitor Alert’ \
> -U stadba -Pdbapwd1 \
> -T 05:00 \
> -i 600 \
> -o /var/log/tbi/db/STAResourceAlerts.csv \
> -n on
```

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

```
Contacting daemon...connected.
Setting DB Tablespace HWM.... 65
Setting DB Disk Volume HWM... 65
Setting Logging Volume HWM... 65
Setting System Memory HWM.... 95
Setting 'From:' address...... STAMonitor@localhost
Setting 'To:' addresses...... STAadmin@MyCompany.com:ABCadmin@MyCompany.com
Setting 'Subject:' line...... STA Resource Monitor Alert
Setting Send Time Hour....... 05:00
Setting Output Filename...... /var/log/tbi/db/STAResourceAlerts.csv
Setting Sleep Interval....... 600
Setting Alert Nag Mode....... ON
Setting DB Username.......... stadba
Setting DB Password.......... *******
Done.
Current STA Resource Monitor Service Settings:
   Configured                 [yes]
   Send Reports         -T [05:00]
   Sleep Interval       -i [600 sec]
   Alert Nagging        -n [on]
   DB Username          -U [stadba]
   DB Password          -P [*******]
   DB Tablespace hwm    -t [65%]
   DB Disk Volume hwm   -d [65%]
   STA Log Volume hwm   -l [65%]
   System Memory hwm    -m [95%]
   Email 'From:'        -f [STAMonitor@localhost]
   Email 'To:'          -r [STAadmin@MyCompany.com:ABCadmin@MyCompany.com]
   Email 'Subject:'     -s [STA Resource Monitor Alert]
   Output File          -o [/var/log/tbi/db/STAResourceAlerts.csv]
===================================================
#
```

4. **Review the command output to verify that the values have been set correctly. If you need to make corrections, you can resubmit just the attributes that need to be changed.**

```
# staresmonadm -i 3600
Contacting daemon...connected.
Setting Sleep Interval....... 3600
Done.
 Current STA Resource Monitor Service Settings:
   Configured                [yes]
   Send Reports         -T [05:00]
   Sleep Interval       -i [3600 sec]
   Alert Nagging        -n [on]
   DB Username          -U [stadba]
   DB Password          -P [*******]
   DB Tablespace hwm    -t [65%]
   DB Disk Volume hwm   -d [65%]
   STA Log Volume hwm   -l [65%]
   System Memory hwm    -m [95%]
   Email 'From:'        -f [STAMonitor@localhost]
   Email 'To:'          -r [STAadmin@MyCompany.com:ABCadmin@MyCompany.com]
   Email 'Subject:'     -s [STA Resource Monitor Alert]
   Output File          -o [/var/log/tbi/db/STAResourceAlerts.csv]
===================================================
#
```

# Services Daemon Task

## ▼ 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. **Restart the STA Services daemon.**

```
# service staservd restart
Restarting STAServer daemon Wed Oct 19 16:10:17 MDT 2011  ...
stopping ... starting ... started [pid=11956]
#
```

2. **Display the status of the daemon to confirm that it is running.**

```
# service staservd status
STAServer daemon is running [pid=11956]
#
```

5

# Configuring STA Identity Management - Local Users and Open LDAP

You must authenticate users to the STA system before they can be allowed access. The actions you take are limited to authorized actions. STA supports using an external SSP to perform authentication and authorization.

When you first connect to the STA system by entering the system URL into your browser, you are prompted for a username and password. When you successfully authenticate, STA checks to make sure you belong to the StorageTapeAnalyticsUser role, and then grants you access.

The following topics are included in this chapter:

- "STA Roles"
- "STA Role Assignment" on page 125
- "Configure WebLogic Local Users" on page 126
- "Configure WebLogic Open LDAP Users" on page 131.

## STA Roles

The Administrator role can be defined in the STA system and can perform all actions allowed to customers.

## STA Role Assignment

STA permits customers to configure an external security service provider (SSP), including:

- local users
- any LDAP-compliant server

When it is configured, STA uses the service provider for authentication and authorization.

If possible, STA creates the STA-specific role in the SSP. An administrator then creates users (if they do not already exist) and assigns them the STA role.

## ▼ Configure WebLogic Local Users

STA supports authenticating and creating local users. Local users are set up in the WebLogic Console and apply to the STA application. To set up the local users:

1. **Point your browser to the WebLogic console login screen.**

   http://*yourHostName*:7001/console/

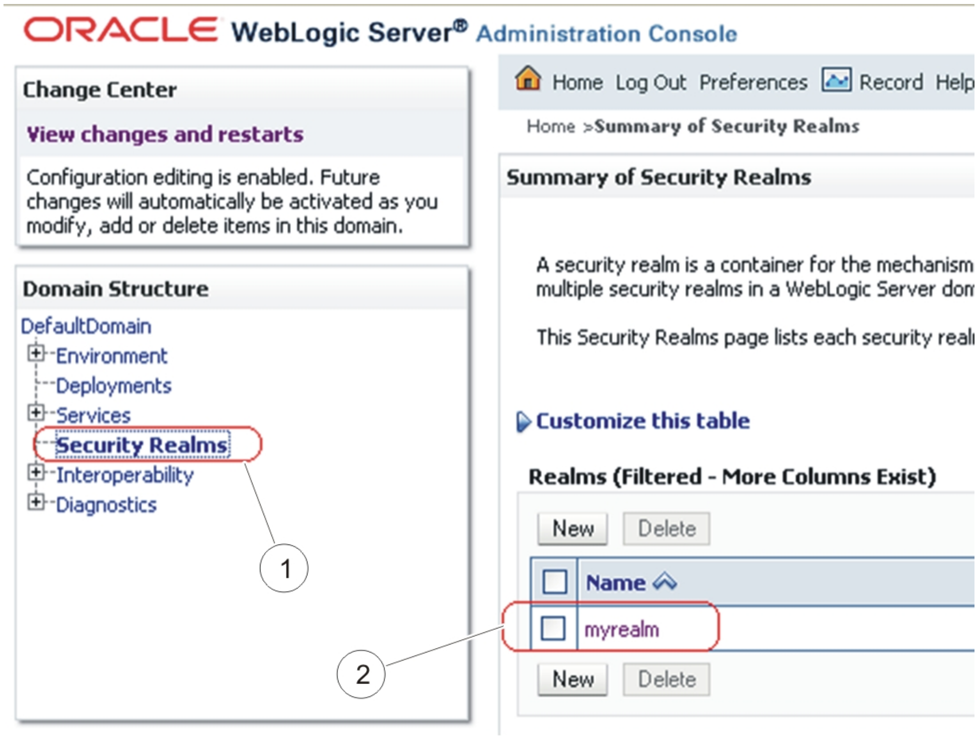
   or

   https://*yourHostName*:7002/console/

   > **Note –** Use the HTTP or HTTPS port number you selected during STA installation.

2. **Log in using the WebLogic Admin Console username and password you defined during STA installation.**

3. **Click Security Realms, and then select myrealm (select the name itself; do not select the check box).**



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

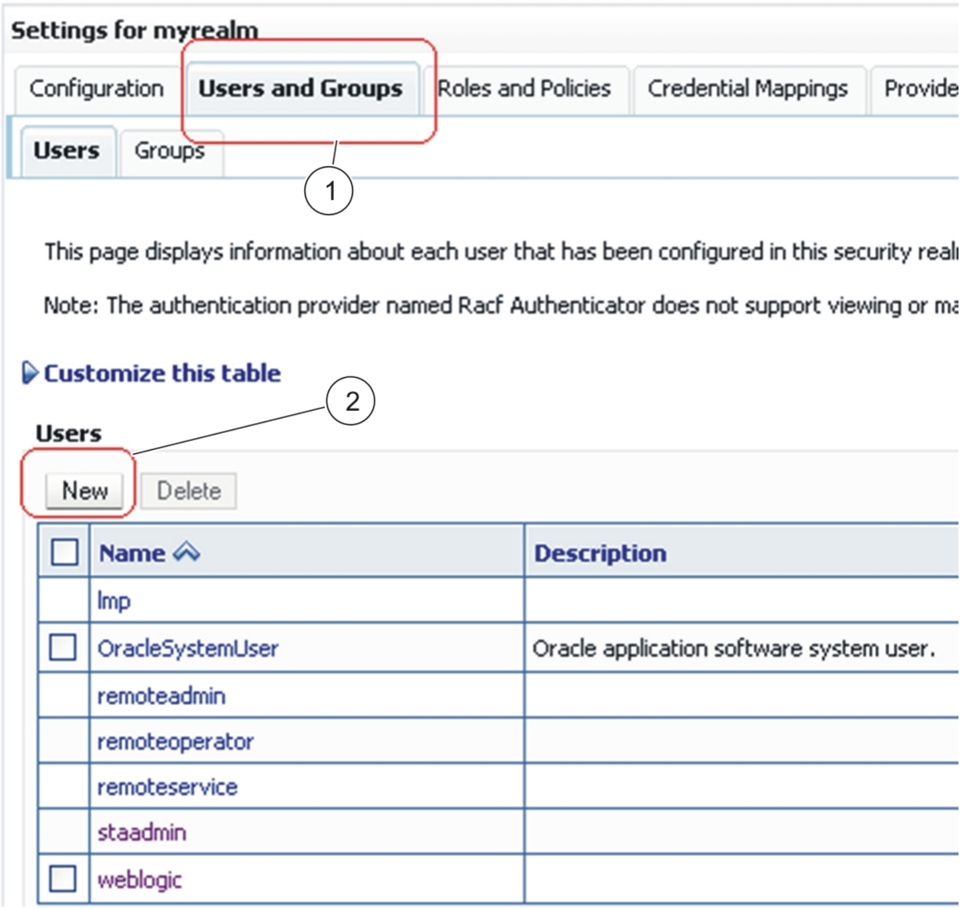
A security realm is a container for the mechanism multiple security realms in a WebLogic Server dor

This Security Realms page lists each security reali

S405_004

1. Security Realms link
2. myrealm link

4. **Click the Users and Groups tab, and then click New.**



This page displays information about each user that has been configured in this security reali

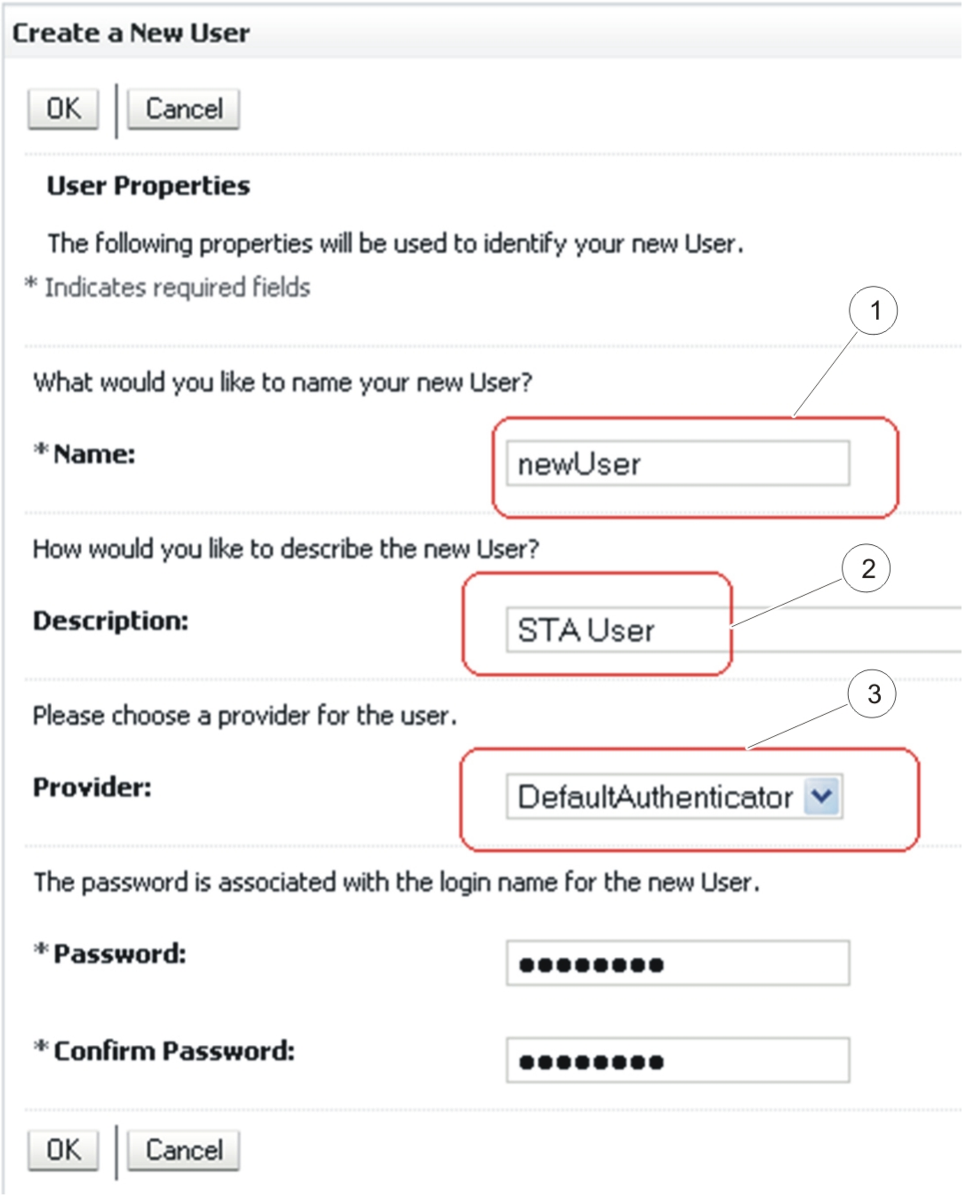
Note: The authentication provider named Racf Authenticator does not support viewing or ma

| ☐ | Name | Description |
|---|---|---|
| | lmp | |
| ☐ | OracleSystemUser | Oracle application software system user. |
| | remoteadmin | |
| | remoteoperator | |
| | remoteservice | |
| | staadmin | |
| ☐ | weblogic | |

S405_005

1. Users and Groups tab
2. New button

**5. Enter a user name, description, and password. Select DefaultAuthenticator from the Provider list and click OK.**



Create a New User

User Properties

The following properties will be used to identify your new User.

* Indicates required fields

What would you like to name your new User?

*Name: newUser

How would you like to describe the new User?

Description: STA User

Please choose a provider for the user.

Provider: DefaultAuthenticator

The password is associated with the login name for the new User.

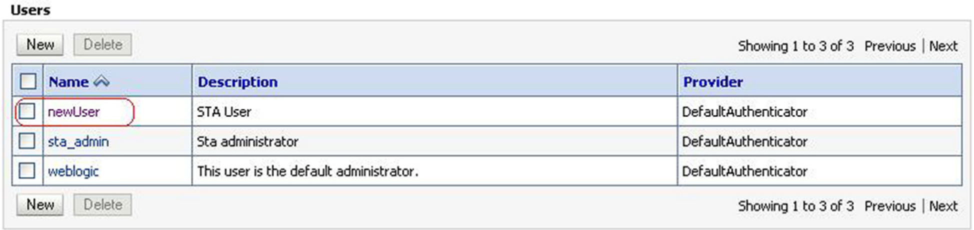
*Password: ●●●●●●●●●

*Confirm Password: ●●●●●●●●●

S405_006

1. User name
2. Description
3. Provider

**6. Click the new username from the list.**



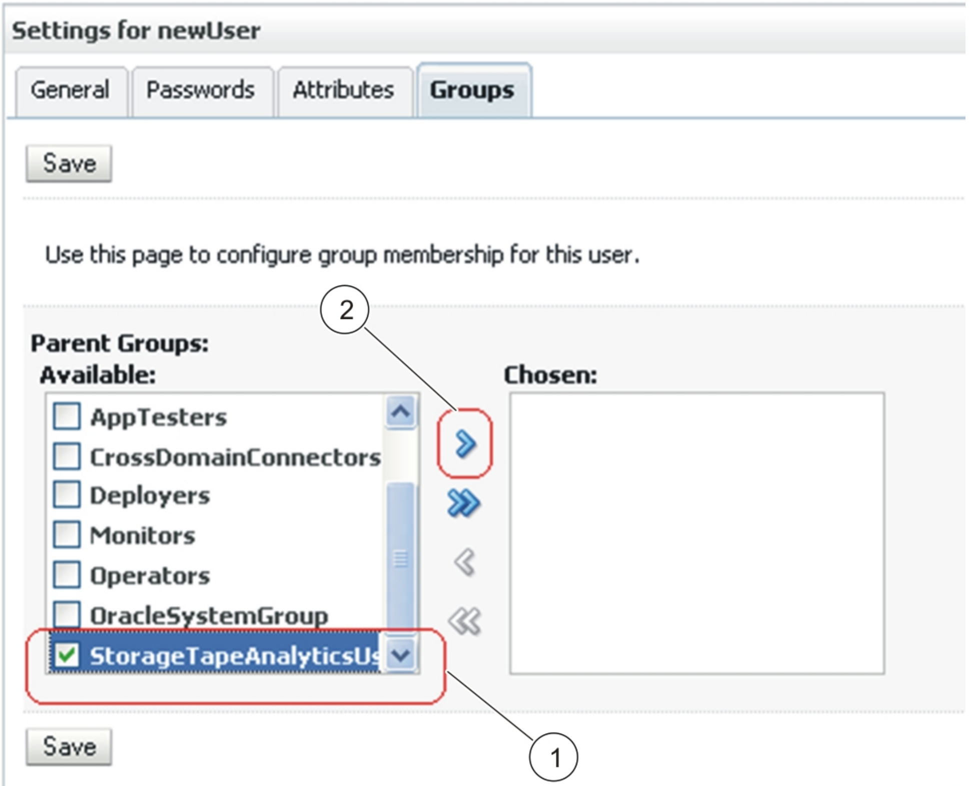
Users

New Delete Showing 1 to 3 of 3 Previous | Next

| □ | Name | Description | Provider |
|---|---|---|---|
| □ | newUser | STA User | DefaultAuthenticator |
| □ | sta_admin | Sta administrator | DefaultAuthenticator |
| □ | weblogic | This user is the default administrator. | DefaultAuthenticator |

New Delete Showing 1 to 3 of 3 Previous | Next

7. **Select the Groups tab. Then, select StorageTapeAnalyticsUser and click the right arrow to move the selection to the right side of the panel.**



Settings for newUser

Use this page to configure group membership for this user.

Parent Groups:

Available:

- □ AppTesters
- □ CrossDomainConnectors
- □ Deployers
- □ Monitors
- □ Operators
- □ OracleSystemGroup
- ☑ StorageTapeAnalyticsUs

Chosen:

S405_011

1. StorageTapeAnalyticsUser parent group
2. Right arrow

8. **Click the Save button.**

You should now be able to log into STA application using the new user login ID.

**Note –** If you would like to add additional WebLogic local users, repeat the previous steps for each additional user, starting with Step 3.

## ▼ Configure WebLogic Open LDAP Users

STA supports authenticating users with Open LDAP. This service, however, must be set up separately from STA, since it is not built directly into the application. To configure Open LDAP for STA, follow the steps below.

> **Note –** You must set up Open LDAP on a separate server.

1. **Point your browser to the WebLogic console login screen.**

   http://*yourHostName*:7001/console/

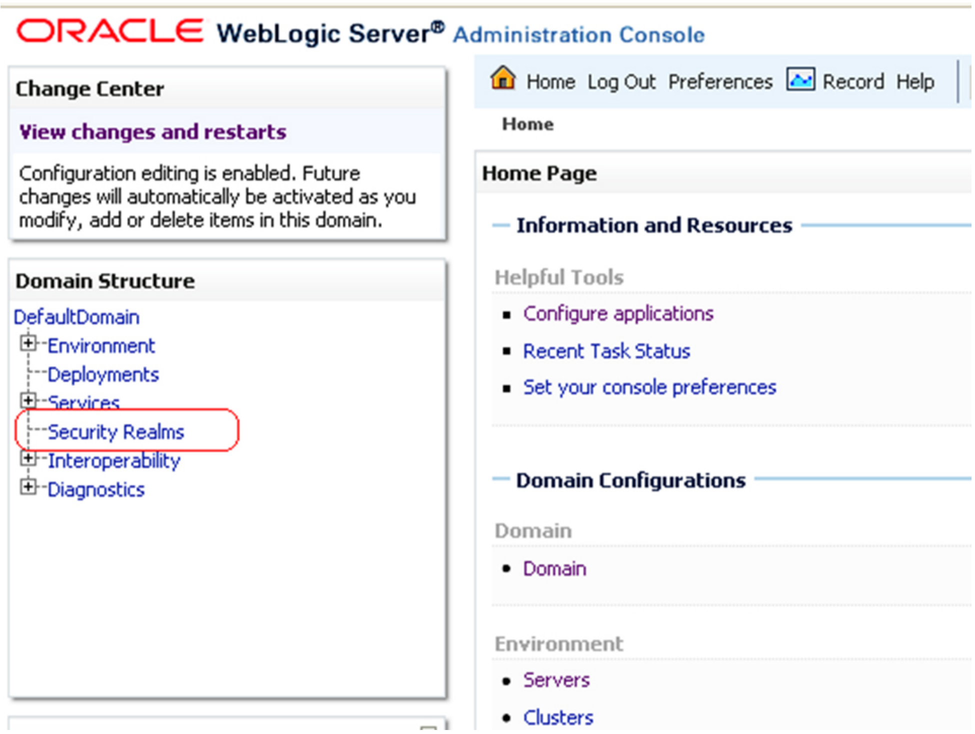
   or

   https://*yourHostName*:7002/console/

   > **Note –** Use the HTTP or HTTPS port number you selected during STA installation.

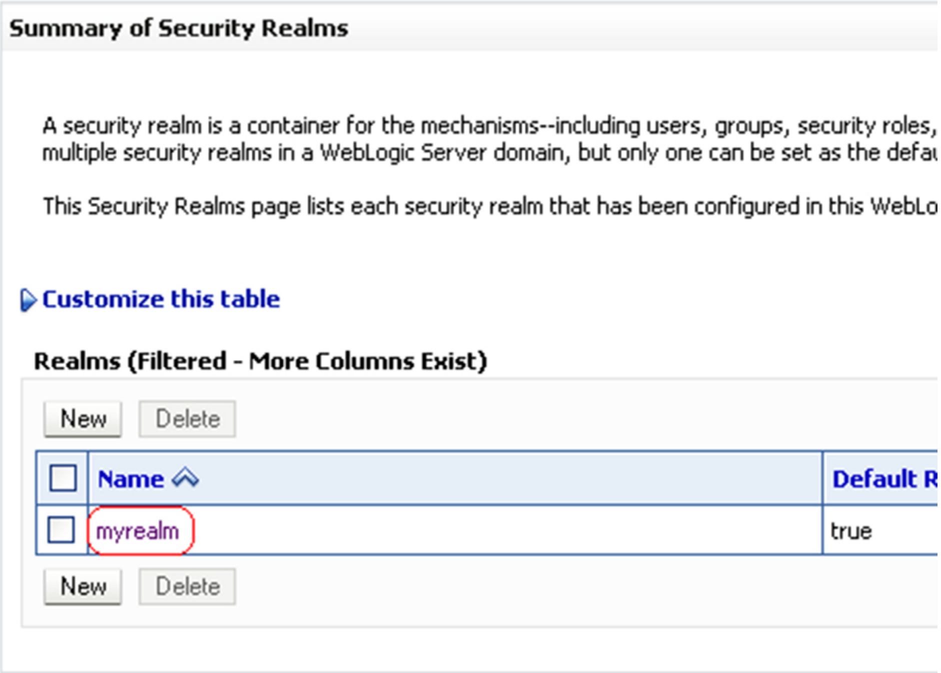
2. **Log in using the WebLogic Admin Console username and password you defined during STA installation.**

3. **Click Security Realms.**



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

4. **Click myrealm (select the name itself, you cannot check the box).**



Summary of Security Realms

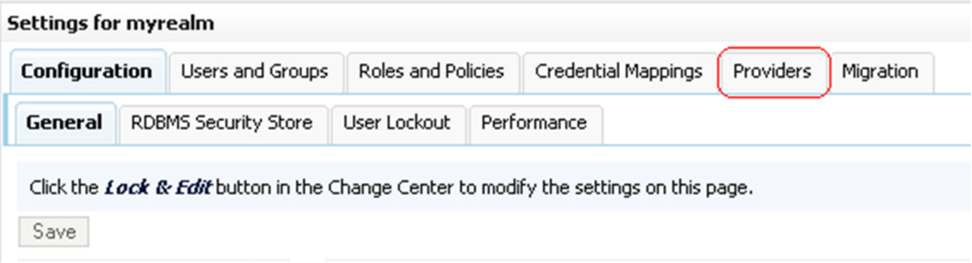
A security realm is a container for the mechanisms--including users, groups, security roles, multiple security realms in a WebLogic Server domain, but only one can be set as the defau

This Security Realms page lists each security realm that has been configured in this WebLo

Realms (Filtered - More Columns Exist)

| □ | Name | Default R |
|---|---|---|
| □ | myrealm | true |

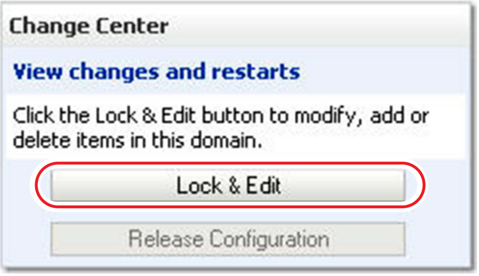
5. Click the Providers tab.



Settings for myrealm

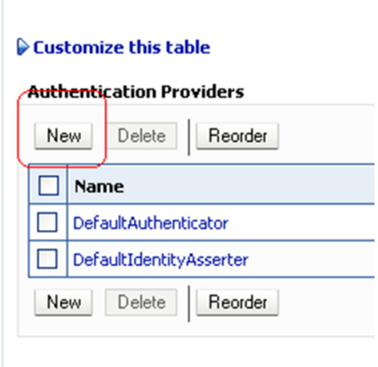
Click the *Lock & Edit* button in the Change Center to modify the settings on this page.

6. Click Lock & Edit.



Click the Lock & Edit button to modify, add or delete items in this domain.

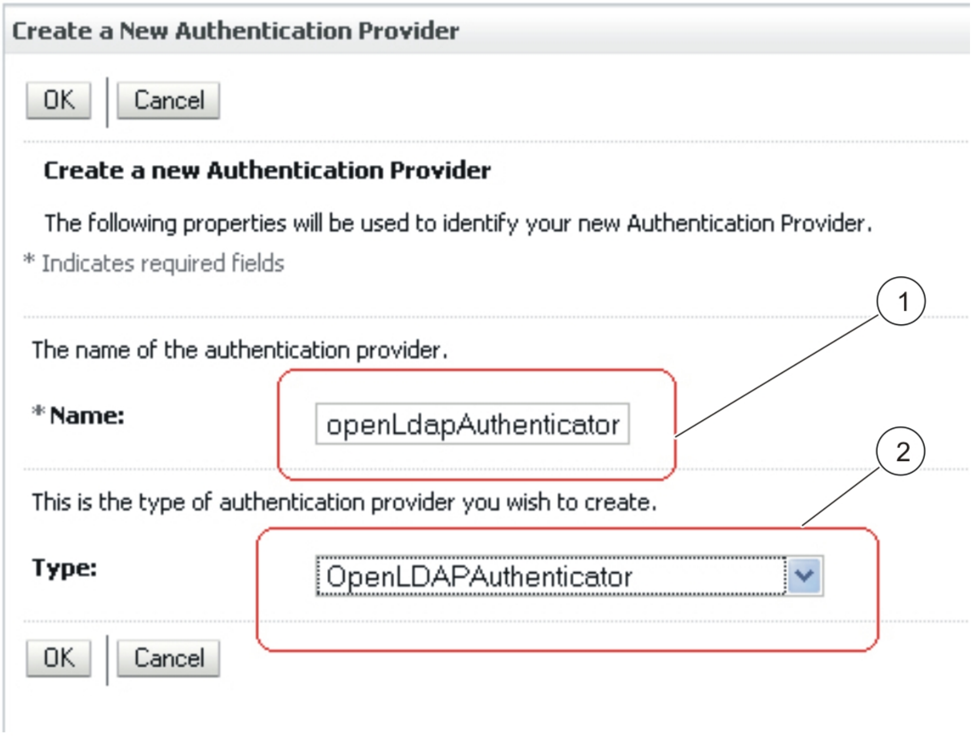
7. **Click New.**



Authentication Providers

| □ | Name |
|---|---|
| □ | DefaultAuthenticator |
| □ | DefaultIdentityAsserter |

8. **Enter the name of the authentication provider and select OpenLDAPAuthenticator in the Type list. Click OK.**



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: openLdapAuthenticator

This is the type of authentication provider you wish to create.

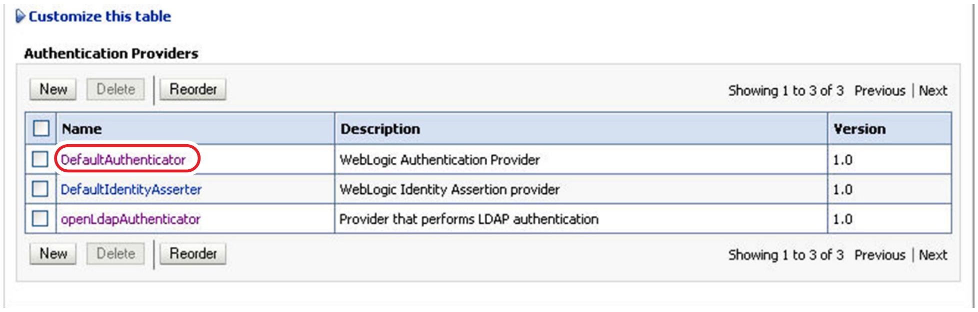
Type: OpenLDAPAuthenticator

OK | Cancel

S405_010

1. Authentication provider name
2. Authentication provider type

9. **Select DefaultAthenticator (select the name itself, you cannot not check the box) and change the Control Flag to Sufficient. Click Save.**



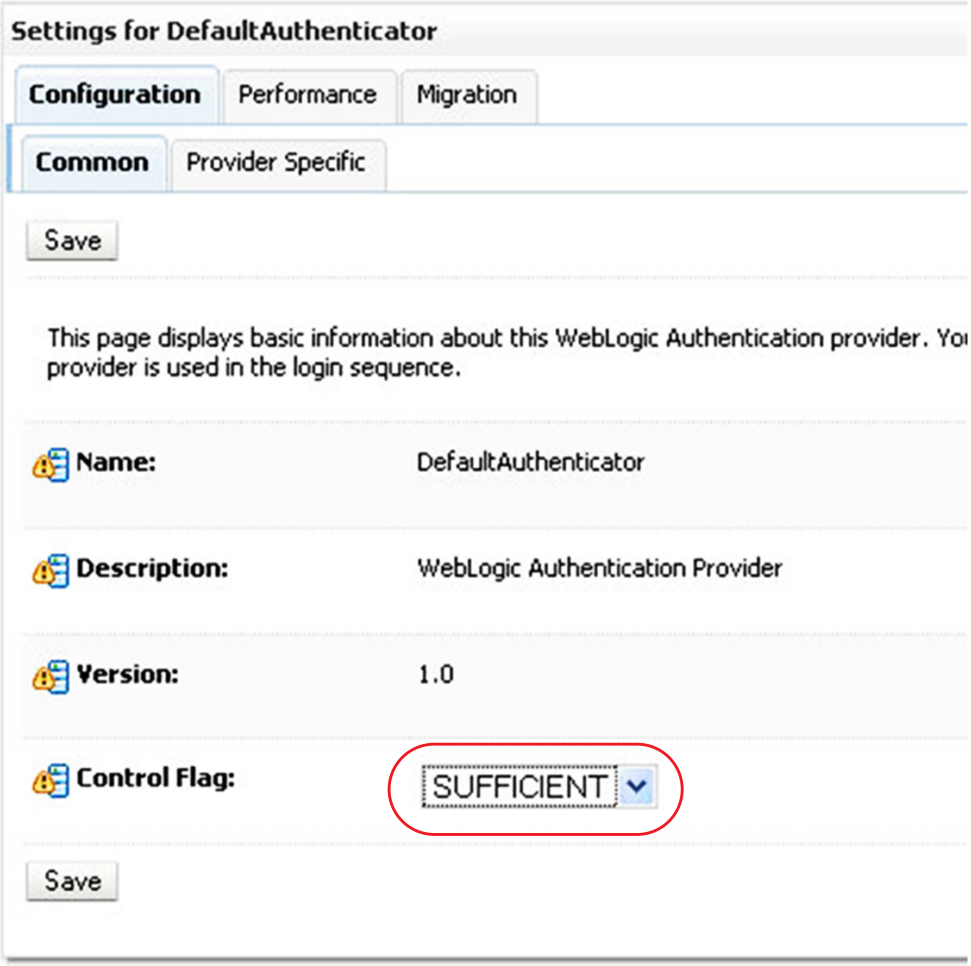
Customize this table

Authentication Providers

New | Delete | Reorder — Showing 1 to 3 of 3 Previous | Next

| □ | Name | Description | Version |
|---|---|---|---|
| □ | DefaultAuthenticator | WebLogic Authentication Provider | 1.0 |
| □ | DefaultIdentityAsserter | WebLogic Identity Assertion provider | 1.0 |
| □ | openLdapAuthenticator | Provider that performs LDAP authentication | 1.0 |

New | Delete | Reorder — Showing 1 to 3 of 3 Previous | Next



Settings for DefaultAuthenticator

This page displays basic information about this WebLogic Authentication provider. Yo
provider is used in the login sequence.

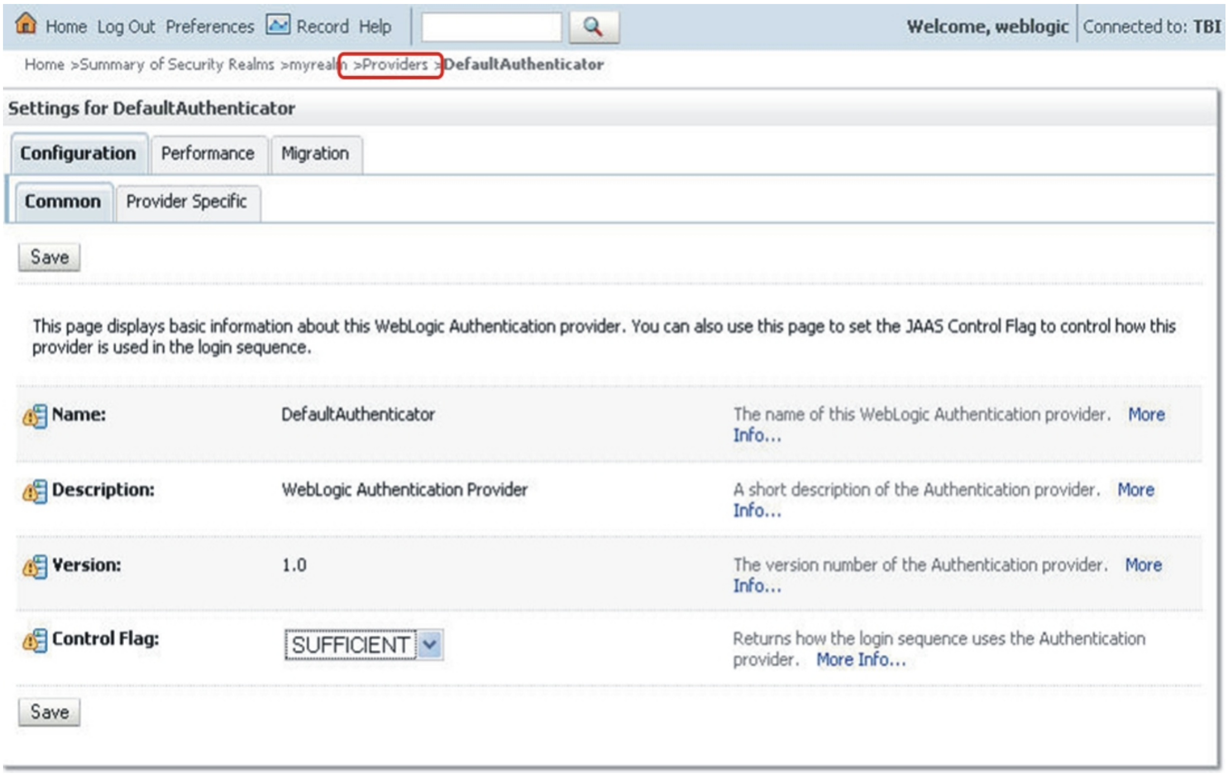
Name: DefaultAuthenticator

Description: WebLogic Authentication Provider

Version: 1.0

Control Flag: SUFFICIENT

10. Click the Providers locator link to return to the Authentication Providers screen.

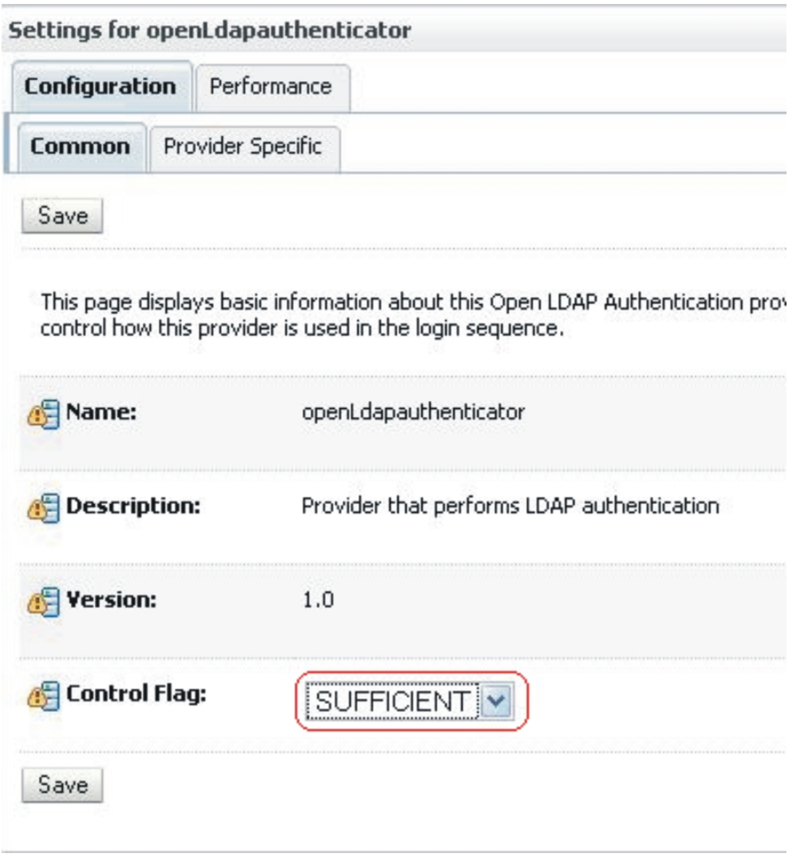

Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: TBI
Home >Summary of Security Realms >myrealm >Providers >DefaultAuthenticator
Configuration
Performance
Migration
Common
Provider Specific
Save
More Info...
Save

Settings for DefaultAuthenticator

This page displays basic information about this WebLogic Authentication provider. You can also use this page to set the JAAS Control Flag to control how this provider is used in the login sequence.

| | | |
|---|---|---|
| Name: | DefaultAuthenticator | The name of this WebLogic Authentication provider. More Info... |
| Description: | WebLogic Authentication Provider | A short description of the Authentication provider. More Info... |
| Version: | 1.0 | The version number of the Authentication provider. More Info... |
| Control Flag: | SUFFICIENT | Returns how the login sequence uses the Authentication provider. More Info... |

11. **Select openLdapauthenticator (select the name itself, you cannot check the box) and change the Control Flag to Sufficient. Click Save.**



Settings for openLdapauthenticator

This page displays basic information about this Open LDAP Authentication pro
control how this provider is used in the login sequence.

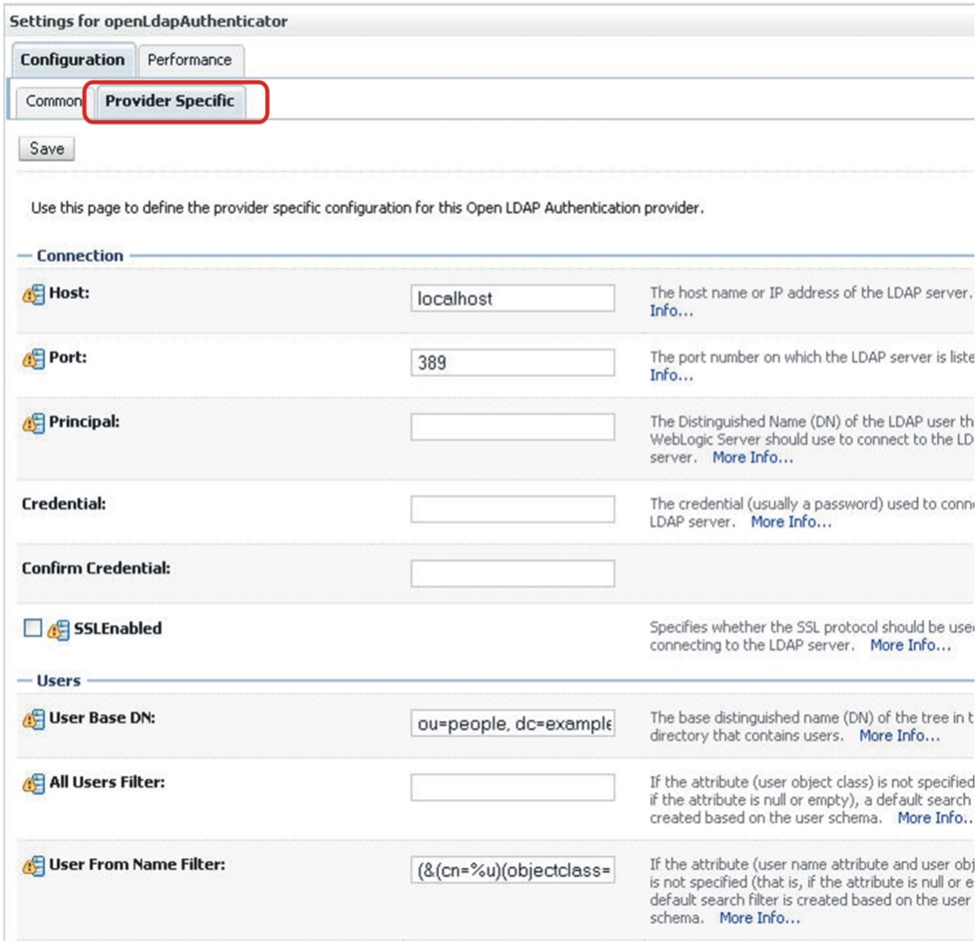
Name: openLdapauthenticator

Description: Provider that performs LDAP authentication

Version: 1.0

Control Flag: SUFFICIENT

12. **Click the Provider Specific secondary tab for the openLdapAuthenticator settings.**



Settings for openLdapAuthenticator

Configuration | Performance

Common | Provider Specific

Save

Use this page to define the provider specific configuration for this Open LDAP Authentication provider.

**Connection**

| | | |
|---|---|---|
| **Host:** | localhost | The host name or IP address of the LDAP server. Info... |
| **Port:** | 389 | The port number on which the LDAP server is liste Info... |
| **Principal:** | | The Distinguished Name (DN) of the LDAP user th WebLogic Server should use to connect to the LD server. More Info... |
| **Credential:** | | The credential (usually a password) used to conn LDAP server. More Info... |
| **Confirm Credential:** | | |
| □ **SSLEnabled** | | Specifies whether the SSL protocol should be use connecting to the LDAP server. More Info... |

**Users**

| | | |
|---|---|---|
| **User Base DN:** | ou=people, dc=example | The base distinguished name (DN) of the tree in t directory that contains users. More Info... |
| **All Users Filter:** | | If the attribute (user object class) is not specified if the attribute is null or empty), a default search created based on the user schema. More Info.. |
| **User From Name Filter:** | (&(cn=%u)(objectclass= | If the attribute (user name attribute and user obj is not specified (that is, if the attribute is null or e default search filter is created based on the user schema. More Info... |

13. **Enter the following parameters, specifying the settings for your specific LDAP server set up.**

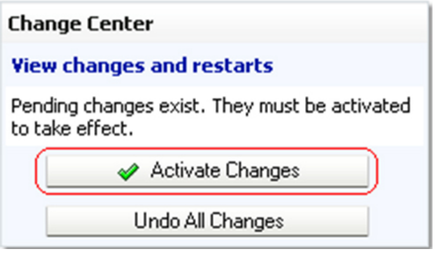
    **The settings below apply to the lses-ldap1 server and are specific to each customer environment.**

    - host = lses-ldap1
    - port = 389
    - Principal = leave blank
    - Credential = leave blank
    - User Base DN = ou=people,dc=oracle,dc=eng
    - User From Name Filter = (&(cn=%u)(objectclass=inetOrgPerson))
    - User Object Class = inetOrgPerson
    - Group Base DN = ou=groups,dc=oracle,dc=eng

- Group From Name Filter = (&(cn=%g)(objectclass=groupofnames))

14. **Click Save.**

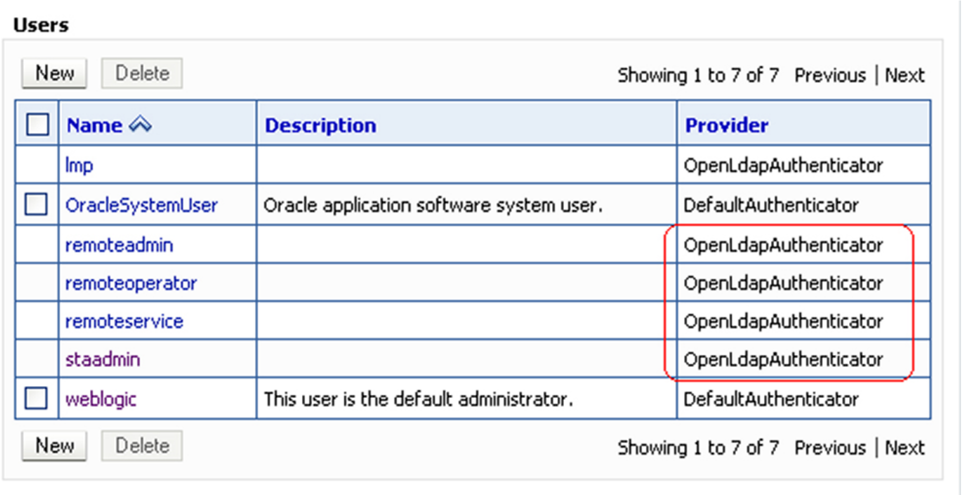
15. **Click Activate Changes.**



Pending changes exist. They must be activated to take effect.

16. **Test the configuration by selecting either the Users or Groups tab under the Security Realms > myrealm > Users and Groups screen. The entries in the example below belong to the openLdapAuthenticator provider.**

    **Note –** You must restart the Admin server in the CLI before running this test. For the command syntax, see the "STA Command" section within the *StorageTek Tape Analytics Administration Reference Guide*.



| ☐ | Name | Description | Provider |
|---|---|---|---|
| | lmp | | OpenLdapAuthenticator |
| ☐ | OracleSystemUser | Oracle application software system user. | DefaultAuthenticator |
| | remoteadmin | | OpenLdapAuthenticator |
| | remoteoperator | | OpenLdapAuthenticator |
| | remoteservice | | OpenLdapAuthenticator |
| | staadmin | | OpenLdapAuthenticator |
| ☐ | weblogic | This user is the default administrator. | DefaultAuthenticator |

17. **Log in to STA using the user that belongs to the StorageTapeAnalyticsUser role (this was set up in LDAP Server during STA Installation).**

# 6

# Configuring STA Identity Management - RACF

This chapter describes the process for installing and configuring STA RACF authorization. The following topics are included:

- “IBM RACF Mainframe Minimum Requirements” on page 142
- “Installing and Configuring STA’s RACF Authorization Facility” on page 142
    - “Enable Mainframe Support for STA RACF Authorization” on page 142
    - “Configure AT-TLS” on page 143
    - “Set Up RACF/SSP for the WebLogic Console” on page 159
    - “Configure SSL Between STA and RACF” on page 160
    - “Configure SSL Between STA and RACF” on page 160
    - “Configure the WebLogic Server” on page 161.

> **Note –** This document refers to the IBM security product, RACF. STA supports third-party products that are compatible with RACF, for example, CA’s ACF-2 and Top Secret. It is up to the person installing STA, or their security administrator, to issue the commands that are appropriate for the security product they have installed on their mainframe, whether it is RACF, ACF-2, Top Secret, or any other product.

# IBM RACF Mainframe Minimum Requirements

If you will use IBM Resource Access Control Facility (RACF) as a method of authentication, the following software and firmware is required.

**TABLE 6-1** IBM RACF Software Required

| Software/Firmware | Version |
|---|---|
| ELS PTFs for STA / RACF | ELS 7.0 - L1H16DH (MVS) |
| **Note**: STA/RACF is NOT supported in HSC 6.2 | ELS 7.1 - L1H16DI (MVS) |
| | ELS 7.2 - in the base code (MVS) |

# Installing and Configuring STA's RACF Authorization Facility

STA supports authenticating users with RACF. The capability for this service, however, must be set up separately from STA, since it is not built directly into the application. You must install two separate packages:

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

## ▼ 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 SMC component 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 as a means of access authentication, you must perform these steps on the mainframe:

1. **Set up an SMC Started Task that runs the HTTP server. You can find details on how to do this in the ELS document** *Configuring and Managing SMC***.**

   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.

2. **Proceed to "Configure AT-TLS" on page 143.**

# ▼ Configure AT-TLS

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.

To implement AT-TLS encryption for the STA to NCS/ELS HTTP server connection, the minimum level needed for the Communication Server is z/OS 1.9. The following available IBM PTFs (for APAR PK69048) should be applied for best performance:

- Release 1A0 : UK39417 available 08/10/07 z/OS 1.10
- Release 190 : UK39419 available 08/10/07 z/OS 1.9

## RACF List Commands

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

## AT-TLS Configuration Process

Perform these tasks to configure AT-TLS:

- "Activate AT-TLS" on page 144
- "Configure the Policy Agent (PAGENT)" on page 144
- "Activate RACF Classes" on page 146
- "Define RACF Keyrings and Certificates" on page 147.

## Activate AT-TLS

1. **Specify the following parameter in the TCPIP profile data set to activate the AT-TLS function:**

```
TCPCONFIG TTLS
```

This statement may be placed in the TCP OBEY file.

## Configure the Policy Agent (PAGENT)

The Policy Agent address space controls which TCP/IP traffic is encrypted.

2. **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)
```

3. **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.

4. **Configure PAGENT.**

For example:

```
TTLSRule          TBI-TO-ZOS
{
   LocalAddr      localtcpipaddress
   RemoteAddr     remotetcpipaddress
   LocalPortRange localportrange
   RemotePortRangeremoteportrange
   Jobname        HTTPserverJobname
   Direction      Inbound
   Priority       255
   TTLSGroupActionRef gAct1~TBI_ICSF
   TTLSEnvironmentActionRefeAct1~TBI_ICSF
   TTLSConnectionActionRef cAct1~TBI_ICSF
}
TTLSGroupAction   gAct1~TBI_ICSF
{
   TTLSEnabled    On
   Trace          2
}
TTLSEnvironmentAction eAct1~TBI_ICSF
{
   HandshakeRole Server
   EnvironmentUserInstance 0
   TTLSKeyringParmsRef keyR~ZOS
}
TTLSConnectionAction cAct1~TBI_ICSF
{
   HandshakeRole  ServerWithClientAuth
   TTLSCipherParmsRef cipher1~AT-TLS__Gold
   TTLSConnectionAdvancedParmsRefcAdv1~TBI_ICSF
   CtraceClearText Off
   Trace          2
}
TTLSConnectionAdvancedParmscAdv1~TBI_ICSF
{
   ApplicationControlled Off
   HandshakeTimeout 10
   ResetCipherTimer 0
   CertificateLabel certificatelabel
   SecondaryMap   Off
}
TTLSKeyringParms  keyR~ZOS
{
   Keyring        keyringname
}
TTLSCipherParms   cipher1~AT-TLS__Gold
{
   V3CipherSuites TLS_RSA_WITH_3DES_EDE_CBC_SHA
   V3CipherSuites TLS_RSA_WITH_AES_128_CBC_SHA
}
```

where:

*localtcpipaddress*

local TCP/IP address (address of HTTP server)

*remotetcpipaddress*

remote TCP/IP address (address of 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 certificate definition

*keyringname*

name from RACF keyring definition

## Activate RACF Classes

5. **Enter the following commands to activate RACF classes. Either the RACF panels or the CLI can be used.**

   The RACF classes include:

- DIGTCERT
- DIGTNMAP
- DIGTRING

SERVAUTH CLASS must be RACLISTed to prevent PORTMAP and RXSERV from abending.

```
SETROPTS RACLIST(SERVAUTH)
RDEFINE SERVAUTH ** UACC(ALTER) OWNER (RACFADM)
RDEFINE STARTED PAGENT*.* OWNER(RACFADM) STDATA(USER(TCPIP)
GROUP(STCGROUP)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)
OWNER(RACFADM)
RDEFINE FACLITY IRR.DIGTCERT.LIST UACC(NONE) OWNER(RACFADM)
RDEFINE FACILITY IRR.DIGTCERT.GENCERT UACC(NONE) OWNER
(RACFADM)
```

## Define RACF Keyrings and Certificates

6. **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.

7. **Enter the following commands to 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('keyingname') DEFAULT USEAGE(PERSONAL)
```

where:

*stcuser*

RACF user id associated with the TCPIP address space

*serverlabel*

Label for the server certificate

*keyringname*

Name of keyring, must match the Keyring specified in the PAGENT configuration

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('clientlabel')
RING('keyingname') USEAGE(PERSONAL)
```

where:

*stcuser*

RACF user id associated with the TCPIP address space

*clientlabel*

Label for the client certificate

*keyringname*

Name of keyring, must match the Keyring specified in the PAGENT configuration

8. **Enter the following commands to 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 8 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.

9. **Proceed to "Create the RACF Profiles" on page 152.**

## ▼ Create the RACF Profiles

1. **Create the RACF profiles to be used by the CGI routine.**

   The profiles are defined in the FACILITY class. The first of the profiles used 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 userid to be added to the SMC.ROLE.STORAGETAPEANALYTICSUSER profile with READ access.

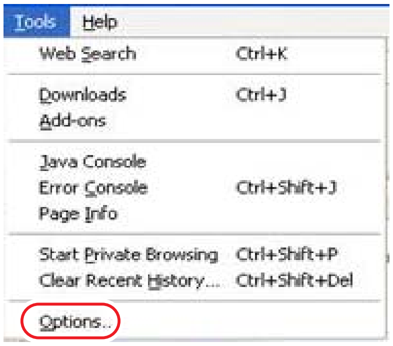
2. **Proceed to "Import the Certificate File and Private Key File" on page 153.**

## ▼ Import the Certificate File and Private Key File

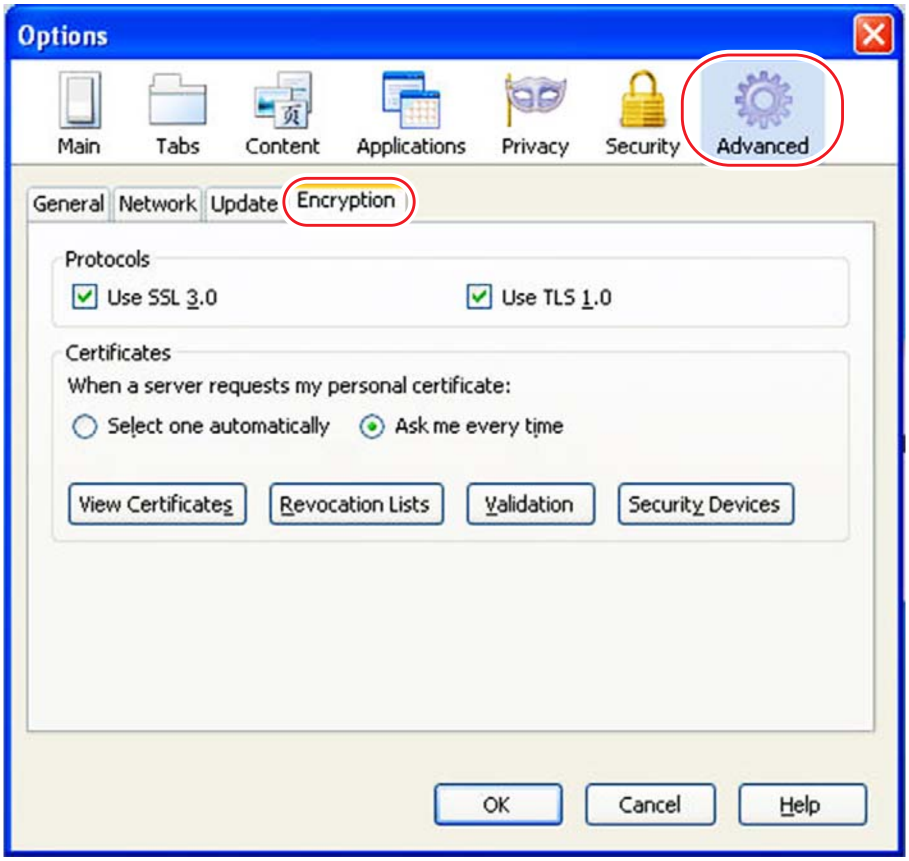
This procedure is optional but can be valuable to test that public and private keys have been generated successfully and that user IDs and passwords with the appropriate permissions have been defined correctly.

The test can be done using any browser, but Firefox is used here as an example.

1. **In Firefox, click Tools and then Options.**


Tools
Help
Web Search Ctrl+K
Downloads Ctrl+J
Add-ons
Java Console
Error Console Ctrl+Shift+J
Page Info
Start Private Browsing Ctrl+Shift+P
Clear Recent History... Ctrl+Shift+Del
Options...

2. **Select the Advanced tab and then the Encryption tab.**



Protocols

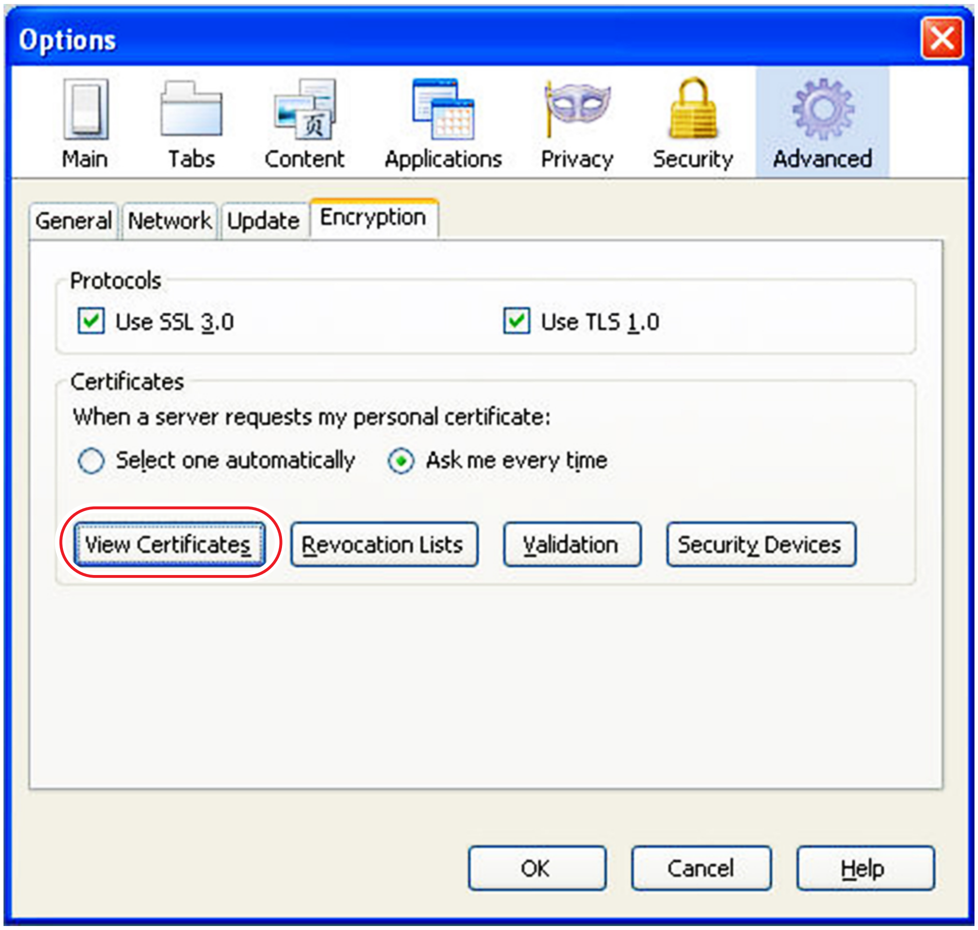
☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

3. **Click the View Certificates button.**



Protocols

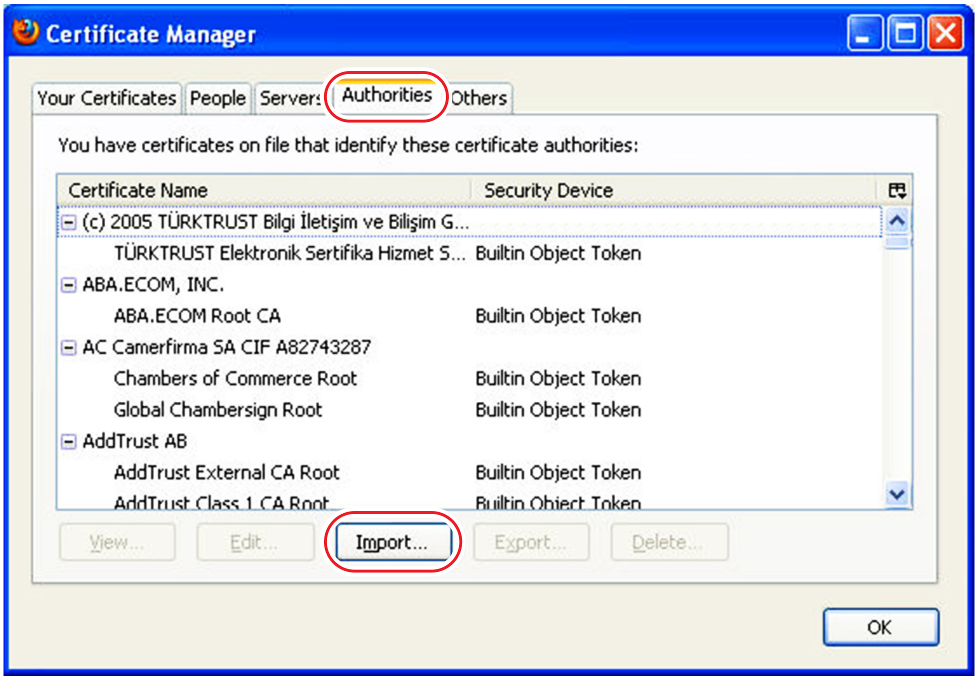
☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

4. **Click the Authorities tab in the Certificate Manager dialog box, and select the certificate file to import.**

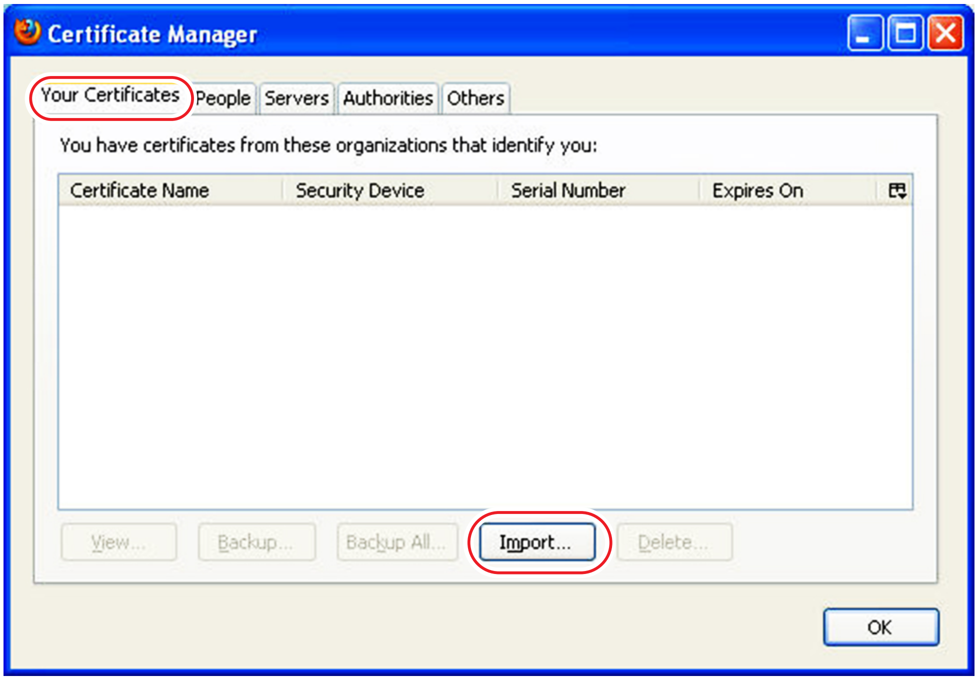


You have certificates on file that identify these certificate authorities:

| Certificate Name | Security Device |
|---|---|
| ⊟ (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim G... | |
| TÜRKTRUST Elektronik Sertifika Hizmet S... | Builtin Object Token |
| ⊟ ABA.ECOM, INC. | |
| ABA.ECOM Root CA | Builtin Object Token |
| ⊟ AC Camerfirma SA CIF A82743287 | |
| Chambers of Commerce Root | Builtin Object Token |
| Global Chambersign Root | Builtin Object Token |
| ⊟ AddTrust AB | |
| AddTrust External CA Root | Builtin Object Token |
| AddTrust Class 1 CA Root | Builtin Object Token |

5. Click Import.

6. Click the Your Certificates tab, and enter the private key file to import.



You have certificates from these organizations that identify you:

7. **Click Import.**
8. **Click the OK button to save and exit the dialog box.**
9. **Proceed to "Test the CGI Routine" on page 158.**

## ▼ Test the CGI Routine

1. **To test the CGI routine from a browser, enter the following URL, where** *host*, *port*, *userid*, **and** *password* **are set to appropriate values.**

   https://*host*:*port*/smcgsaf?type=authentication&userid=*userid*
   &password=*password*&roles=StorageTapeAnalyticsUser

   The resultant 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.

2. **Proceed to “Set Up RACF/SSP for the WebLogic Console” on page 159.**

## ▼ Set Up RACF/SSP for the WebLogic Console

The RACF Security Service Provider (or RACF SSP) must be installed as a plug-in into WebLogic.

To set up RACF:

1. **If the RACF SSP has been installed, the STA installer should put the RACF SSP in the appropriate location within WebLogic. If it has not been installed, place the RACF security `jar` file into the directory named:**

   ```
   /Oracle/Middleware/wlserver_10.3/server/lib/mbeantypes/
   staRACF.jar
   ```

2. **Proceed to "Configure SSL Between STA and RACF" on page 160.**

## ▼ Configure SSL Between STA and RACF

1. **Install the required PTFs on the MVS system. These PTFs allow for authentication with RACF or other third-party security software when you are logging on to the STA.**

- ELS 7.0 - L1H16DH (MVS)
- ELS 7.1 - L1H16DI (MVS)
- ELS 7.2 - in the base code (MVS)

The Application Transparent TLS (AT-TLS) has been configured on MVS so that the port number defined to the SMC HTTP Server and WebLogic is encrypted to the server.

You possess two files: the MVS server certificate (in ASCII format) and the STA client private key (in binary PKCS12 format). The MVS system administrator has given you the password to the PKCS12 file.

2. **Using the Java keytool command, import the certificate file into the `/Oracle/Middleware/jdk1.6.0_xx/jre/lib/security/cacerts` file with the following command:**

```
/Oracle/Middleware/jdkl1.6.0_xx/jre/bin/keytool -importcert -
alias tbiServer -file certificate -keystore /Oracle/Middleware/
jdk1.6.0_xx/jre/lib/security/cacerts -storetype jks
```

3. **Enter the password, and enter Yes to the Trust this certificate? prompt.**

> **Note –** The default password for the `caerts` file is "changeit." **You must change this password.** If you do not, you may be at risk of a security violation.

```
Enter keystore password:xxxxxxxxxx
...
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

4. **Place the private key file in `/opt/oracle/sta/etc`.**

5. **Proceed to "Configure the WebLogic Server" on page 161.**

## ▼ Configure the WebLogic Server

> **Caution –** You must remember the WebLogic administration account usernames and passwords you establish in this procedure. If you forget the usernames or passwords, you must re-install STA.

1. **Point your browser to the WebLogic console login screen.**

   http://*yourHostName*:7001/console/

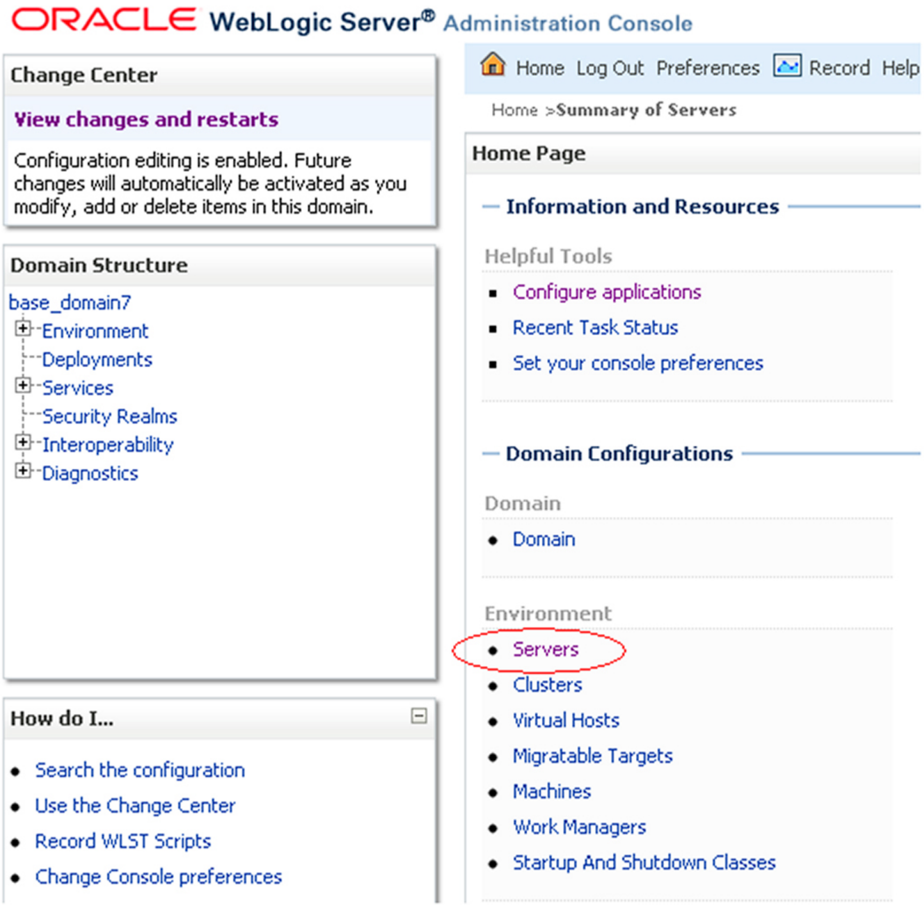
   or

   https://*yourHostName*:7002/console/

   > **Note –** Use the HTTP or HTTPS port number you selected during STA installation.

2. **Log in using the WebLogic Admin Console username and password you defined during STA installation.**

3. **On the home page, select Servers.**



Home >Summary of Servers

**Change Center**

**View changes and restarts**

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

**Domain Structure**

base_domain7
- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

**How do I...**

- Search the configuration
- Use the Change Center
- Record WLST Scripts
- Change Console preferences

**Home Page**

**Information and Resources**

Helpful Tools

- Configure applications
- Recent Task Status
- Set your console preferences

**Domain Configurations**

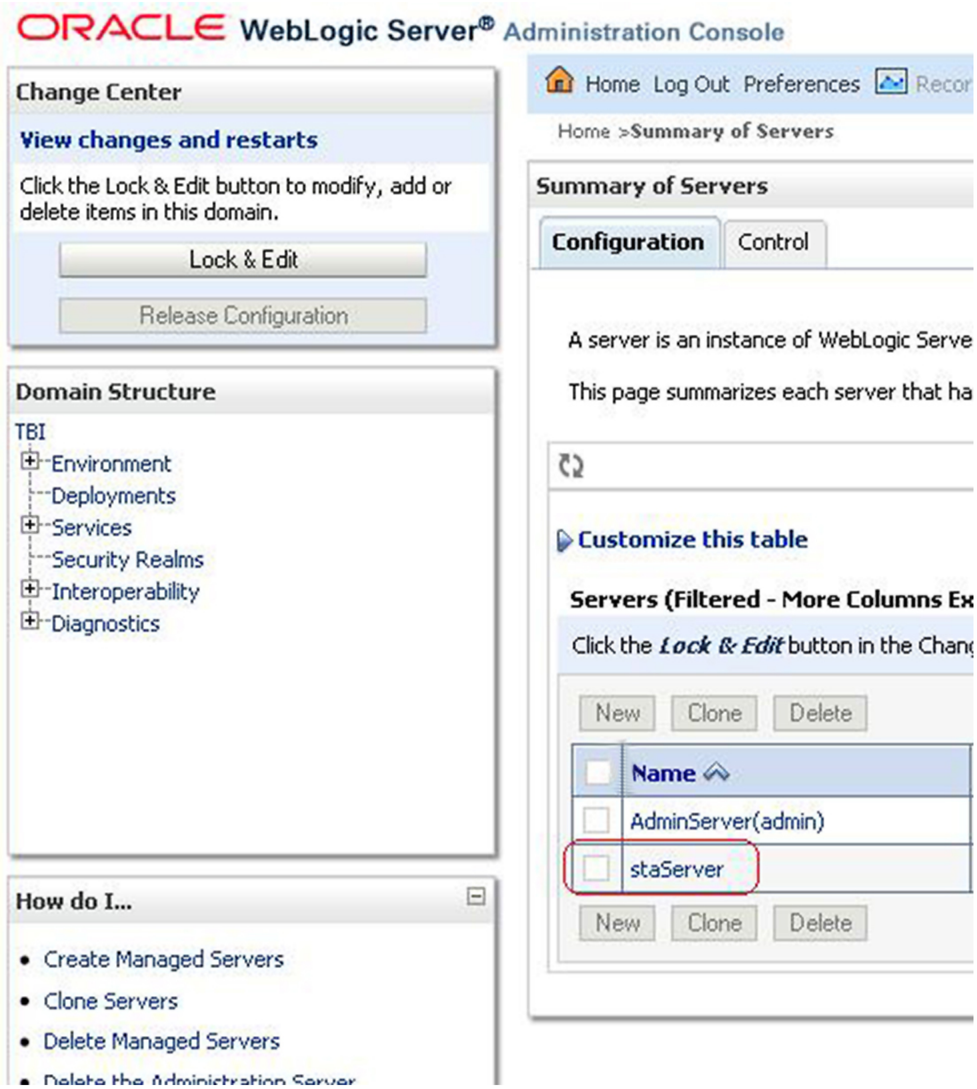
Domain

- Domain

Environment

- Servers
- Clusters
- Virtual Hosts
- Migratable Targets
- Machines
- Work Managers
- Startup And Shutdown Classes

4. **On the Summary of Servers page, select staServer (select the name itself; you cannot check the box).**



Click the Lock & Edit button to modify, add or delete items in this domain.

A server is an instance of WebLogic Serve

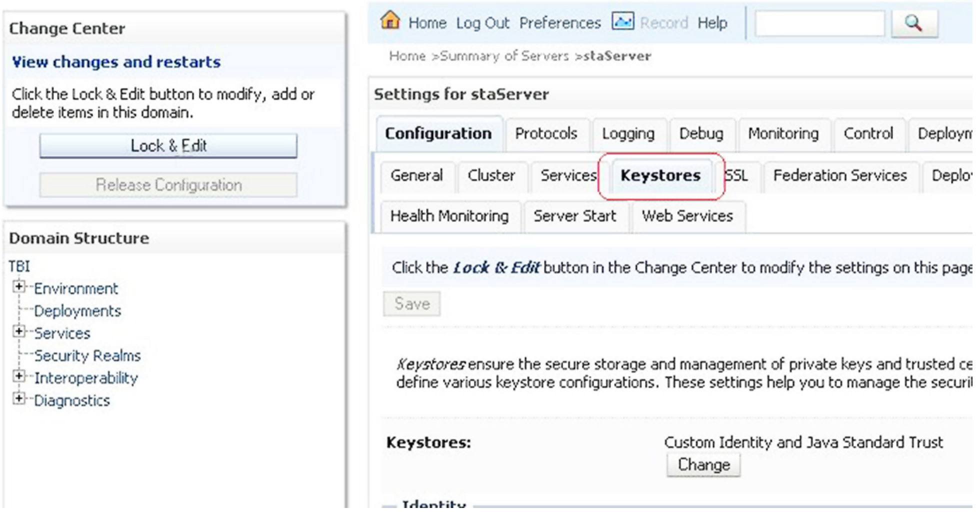
This page summarizes each server that ha

Servers (Filtered - More Columns Ex

Click the *Lock & Edit* button in the Chan

| | Name |
|---|---|
| □ | AdminServer(admin) |
| □ | staServer |

5. **On the Settings for staServer screen, click the Keystores secondary tab.**



Change Center
View changes and restarts
Lock & Edit
Release Configuration
Domain Structure
TBI
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
Home Log Out Preferences Record Help
Home >Summary of Servers >staServer
Settings for staServer
Configuration Protocols Logging Debug Monitoring Control Deploym
General Cluster Services Keystores SSL Federation Services Deplo
Health Monitoring Server Start Web Services
Save
Change
Identity

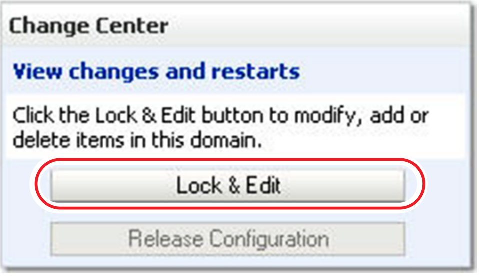
Click the Lock & Edit button to modify, add or delete items in this domain.

Click the *Lock & Edit* button in the Change Center to modify the settings on this page

*Keystores* ensure the secure storage and management of private keys and trusted ce define various keystore configurations. These settings help you to manage the securi

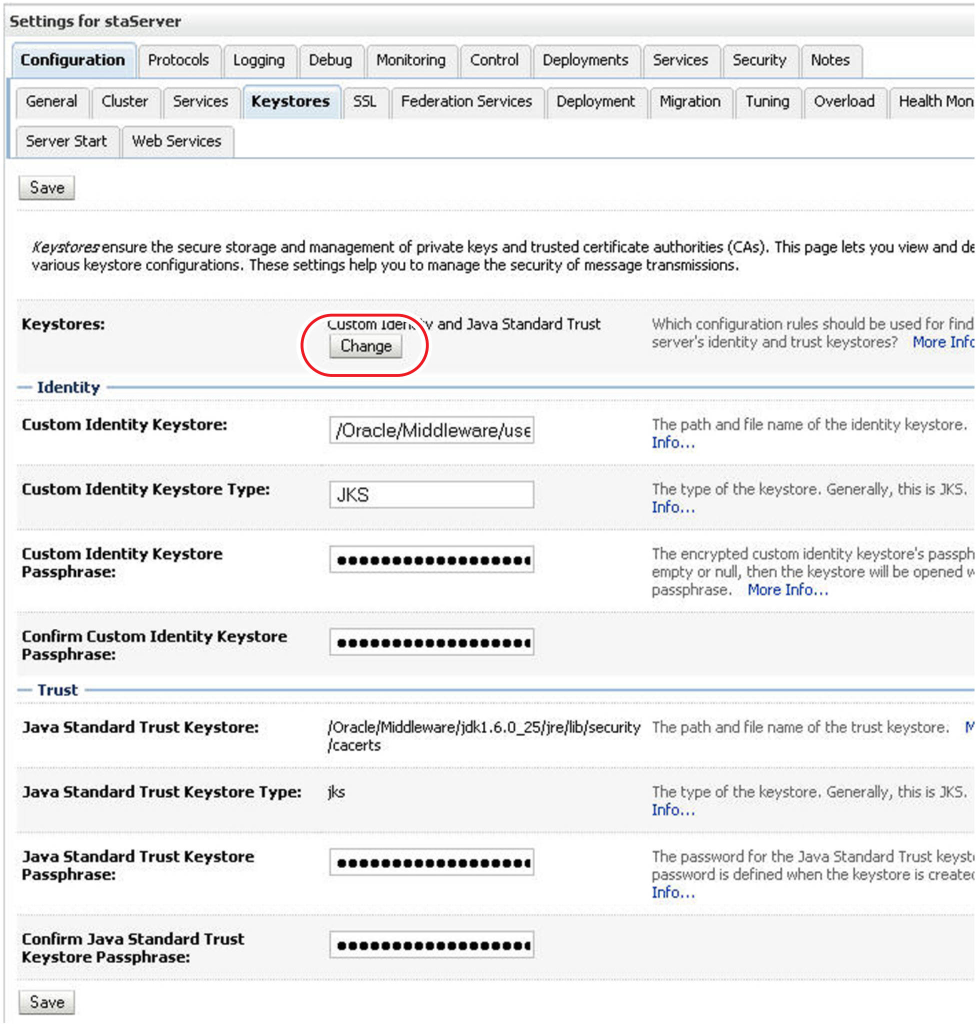
Keystores: Custom Identity and Java Standard Trust

6. **Click Lock & Edit.**



Click the Lock & Edit button to modify, add or delete items in this domain.

7. **On the Keystores page, click Change under Custom Identity and Java Standard Trust.**

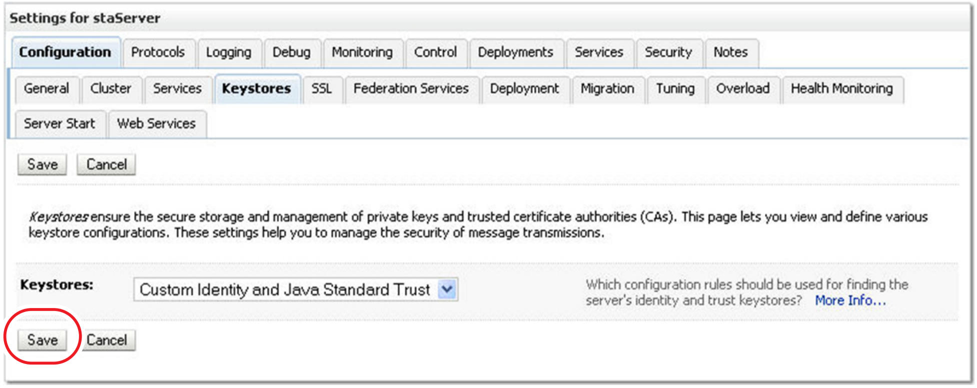


Settings for staServer

*Keystores* ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and de 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 find server's identity and trust keystores? More Info |
| **— Identity** | | |
| **Custom Identity Keystore:** | /Oracle/Middleware/use | The path and file name of the identity keystore. Info... |
| **Custom Identity Keystore Type:** | JKS | The type of the keystore. Generally, this is JKS. Info... |
| **Custom Identity Keystore Passphrase:** | ••••••••••••••••••• | The encrypted custom identity keystore's passph empty or null, then the keystore will be opened w passphrase. More Info... |
| **Confirm Custom Identity Keystore Passphrase:** | ••••••••••••••••••• | |
| **— Trust** | | |
| **Java Standard Trust Keystore:** | /Oracle/Middleware/jdk1.6.0_25/jre/lib/security /cacerts | The path and file name of the trust keystore. M |
| **Java Standard Trust Keystore Type:** | jks | The type of the keystore. Generally, this is JKS. Info... |
| **Java Standard Trust Keystore Passphrase:** | ••••••••••••••••••• | The password for the Java Standard Trust keyst password is defined when the keystore is create Info... |
| **Confirm Java Standard Trust Keystore Passphrase:** | ••••••••••••••••••• | |

8. **Click Save.**



Settings for staServer

*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...

9. **On the Keystores page, enter:**

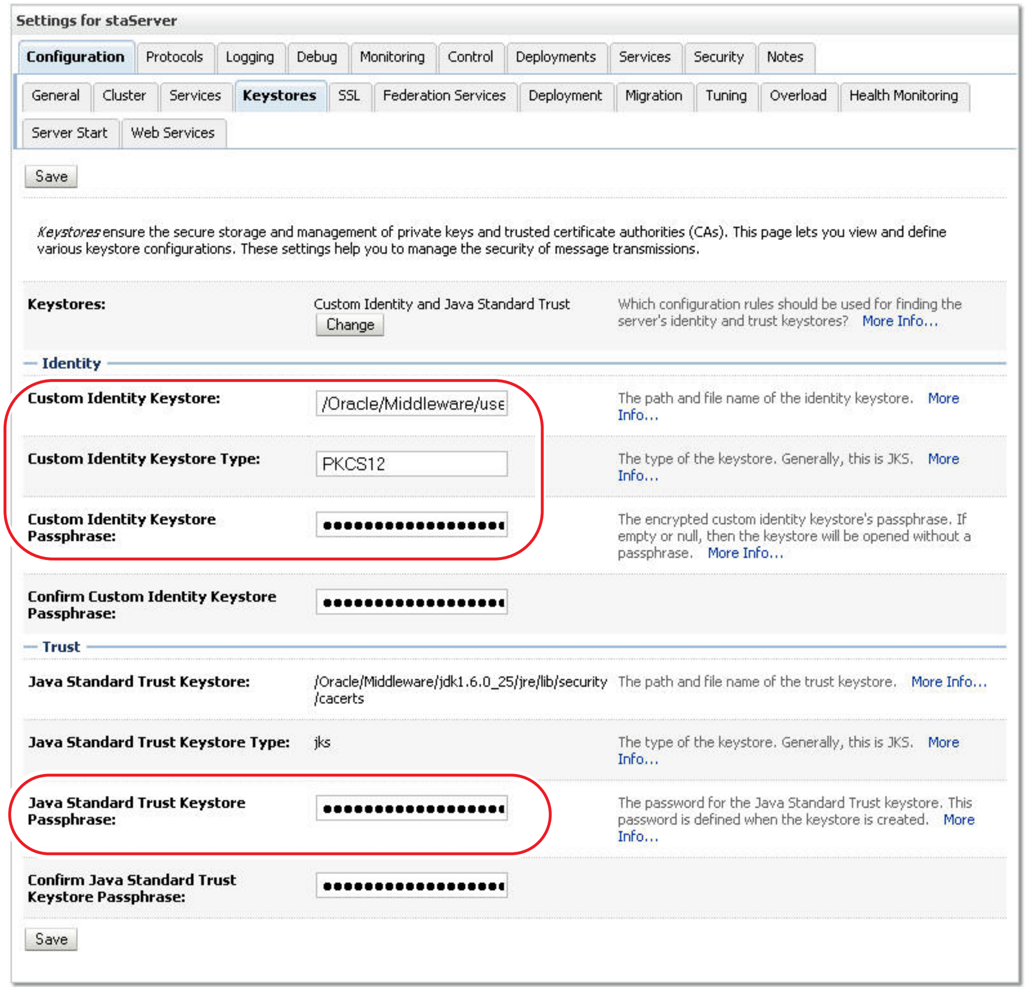
   a. **the path and file of the private key file**

   b. **PKCS12 for the Keystore Type**

   c. **the passphrase supplied by the MVS system administrator**

   d. **the new passphrase for the Java Standard Trust Keystore file (do not enter changeit).**

      **Caution –** You must remember the WebLogic administration account usernames and passwords you enter. If you forget the usernames or passwords, you must re-install STA.



*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...

**Identity**

**Custom Identity Keystore:** /Oracle/Middleware/use — The path and file name of the identity keystore. More Info...

**Custom Identity Keystore Type:** PKCS12 — 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:** /Oracle/Middleware/jdk1.6.0_25/jre/lib/security/cacerts — The path and file name of the trust keystore. More Info...

**Java Standard Trust Keystore Type:** jks — 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...

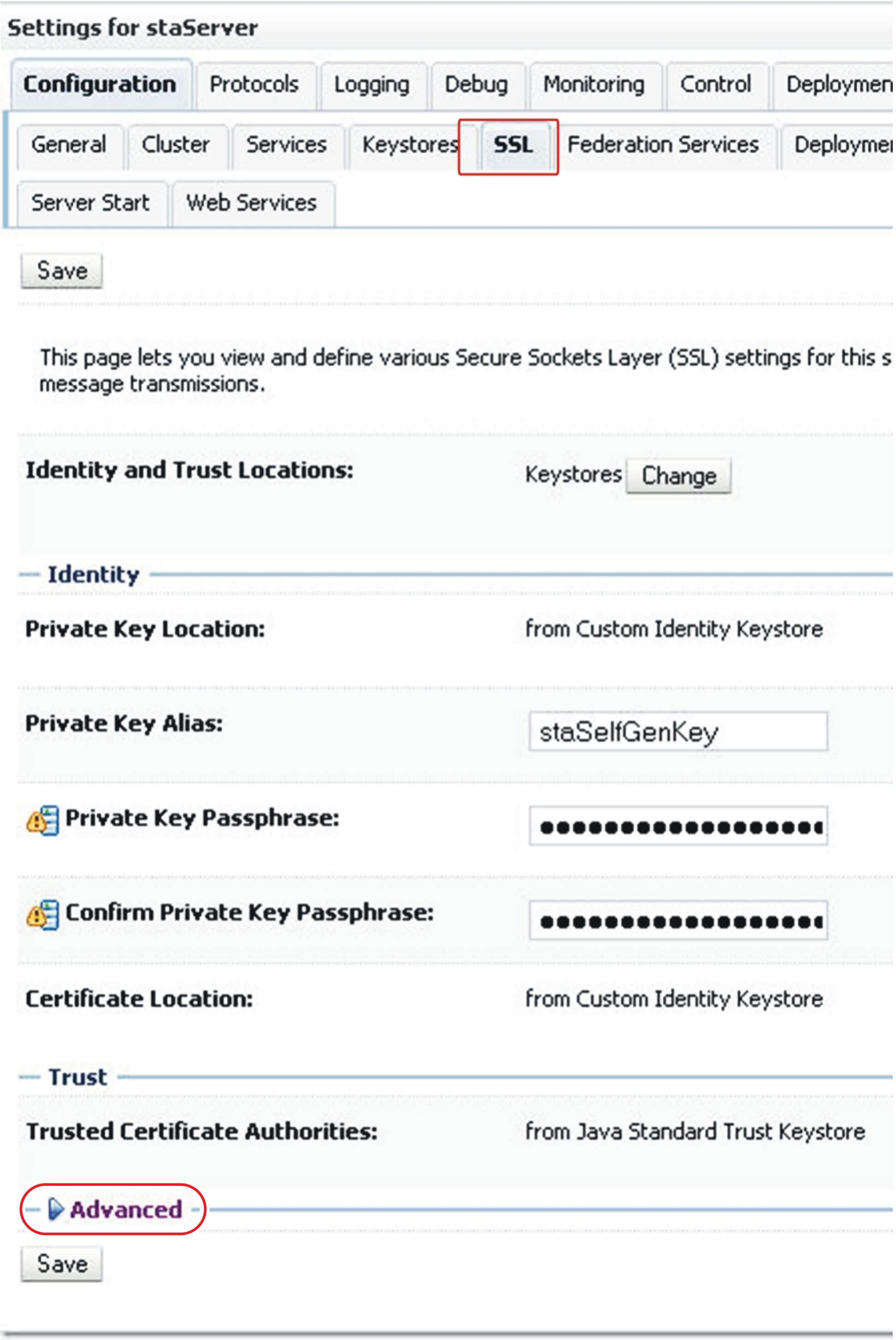
**Confirm Java Standard Trust Keystore Passphrase:** ●●●●●●●●●●●●●●●●●●

10. **Click Save.**

11. **Select the SSL tab, enter the Private Key Alias and the password supplied by the MVS system programmer.**

    **To determine the Private Key Alias, use the `keytool` command.** For example:

```
C:\Temp>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
```



Settings for staServer

This page lets you view and define various Secure Sockets Layer (SSL) settings for this s message transmissions.

Identity and Trust Locations: Keystores

Identity

Private Key Location: from Custom Identity Keystore

Private Key Alias: staSelfGenKey

Private Key Passphrase: ••••••••••••••••••

Confirm Private Key Passphrase: ••••••••••••••••••

Certificate Location: from Custom Identity Keystore

Trust

Trusted Certificate Authorities: from Java Standard Trust Keystore

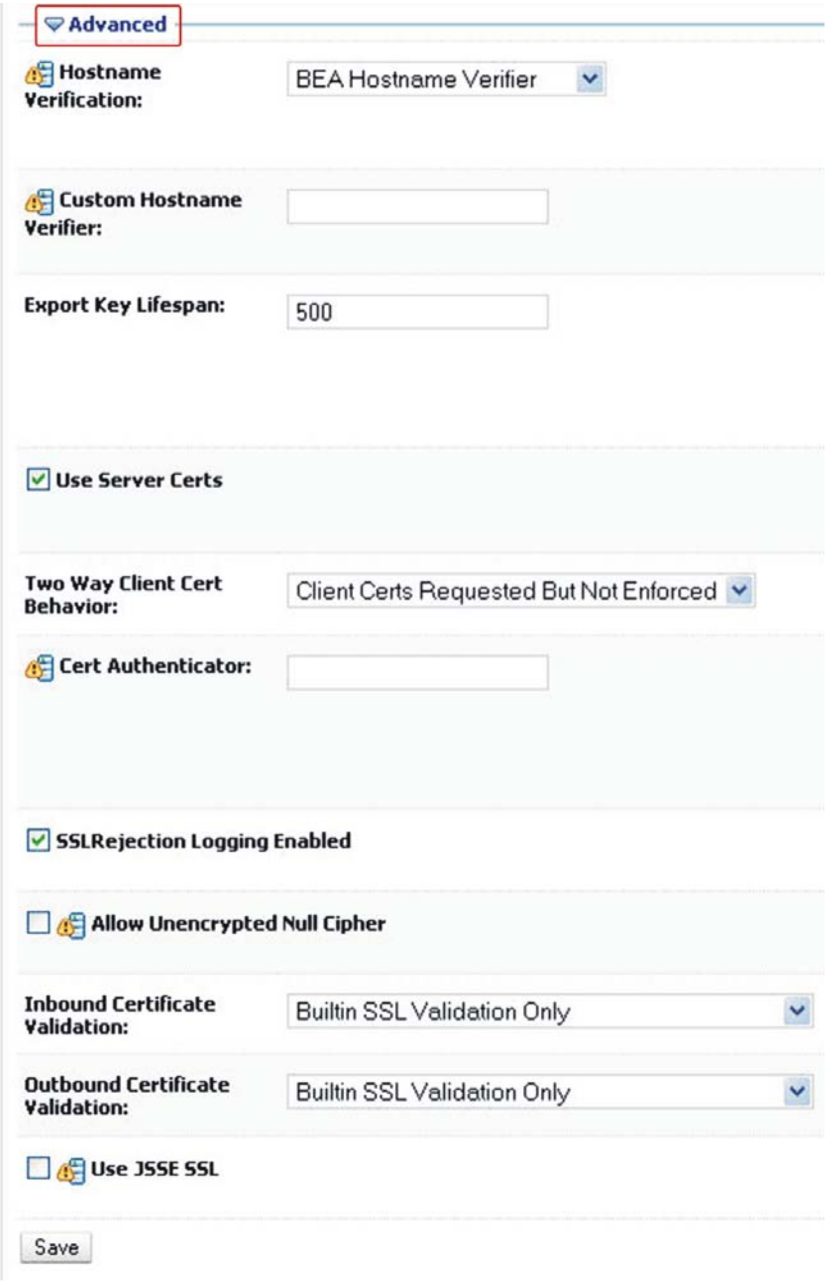
12. Click the Advanced link.

13. Modify the following information:

a. **Check the Use Server Certs field.**

b. **Change the Two Way Client Cert Behavior field list to Client Certs Requested and Enforced.**

c. **Select Builtin SSL Validation and Cert Path Validators for both the Inbound Certification Validation and Outbound Certificate Validation fields.**



Advanced

Hostname Verification: BEA Hostname Verifier

Custom Hostname Verifier:

Export Key Lifespan: 500

☑ Use Server Certs

Two Way Client Cert Behavior: Client Certs Requested But Not Enforced

Cert Authenticator:

☑ SSLRejection Logging Enabled

□ Allow Unencrypted Null Cipher

Inbound Certificate Validation: Builtin SSL Validation Only

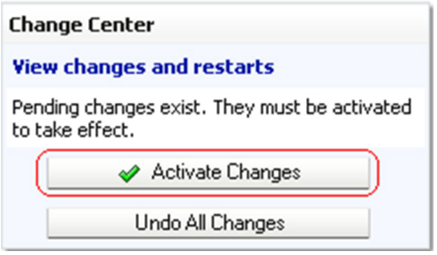
Outbound Certificate Validation: Builtin SSL Validation Only

□ Use JSSE SSL

Save

14. **Click Save.**

15. **Click Activate Changes.**



Change Center

View changes and restarts

Pending changes exist. They must be activated to take effect.

16. **Log out of WebLogic.**

17. **Stop and restart STA.**

```
# STA stop
Stopping the WebLogic staServer....
Successfully stopped the WebLogic staServer
Stopping the WebLogic Administration Server....
Successfully stopped the WebLogic Administration Server
Stopping the STA Database Server Backup Service (staservd)....
Successfully stopped the STA Database Server Backup Service
Stopping the STA database Server....
Successfully stopped the STA Database Server

# STA start
Starting STA Database....
Successfully started the STA Database
Starting STA Database Backup Service (staservd)....
Successfully started the STA Database Backup Service
Starting WebLogic Administration Server....
Successfully started the WebLogic Administration Server
Starting WebLogic staServer....
Successfully started the WebLogic staServer
```

18. **Log in using your username and password.**

19. **Proceed to "Install RACF/SSP on the WebLogic Console" on page 171.**

## ▼ Install RACF/SSP on the WebLogic Console

To install RACF on the WebLogic Console:

1. **Point your browser to the WebLogic console login screen.**

   http://*yourHostName*:7001/console/

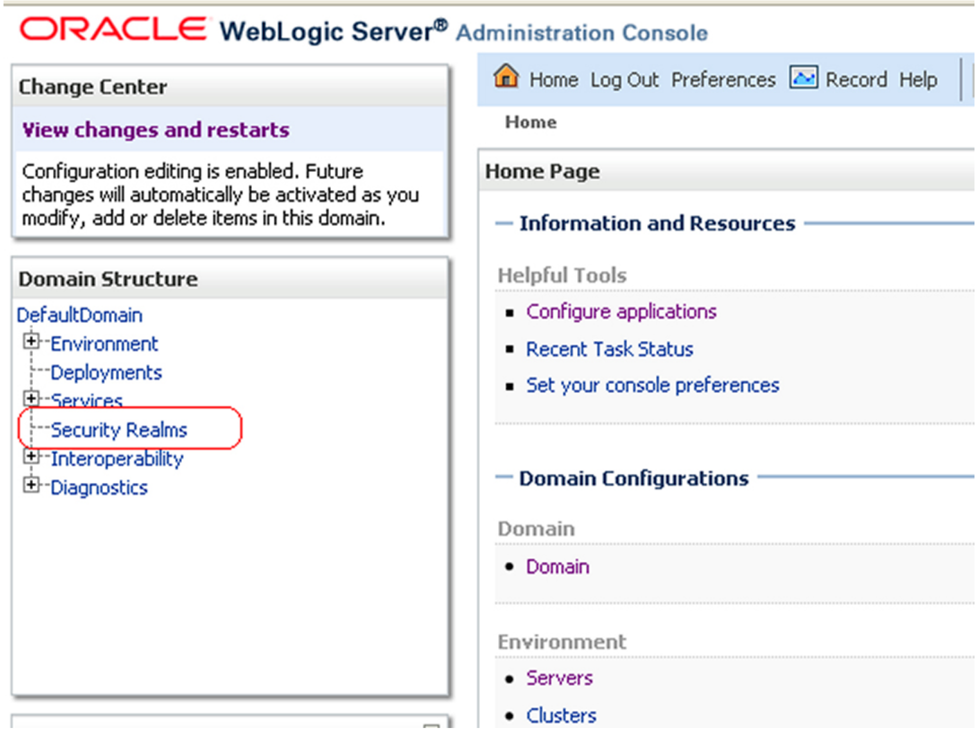
   or

   https://*yourHostName*:7002/console/

   > **Note –** Use the HTTP or HTTPS port number you selected during STA installation.

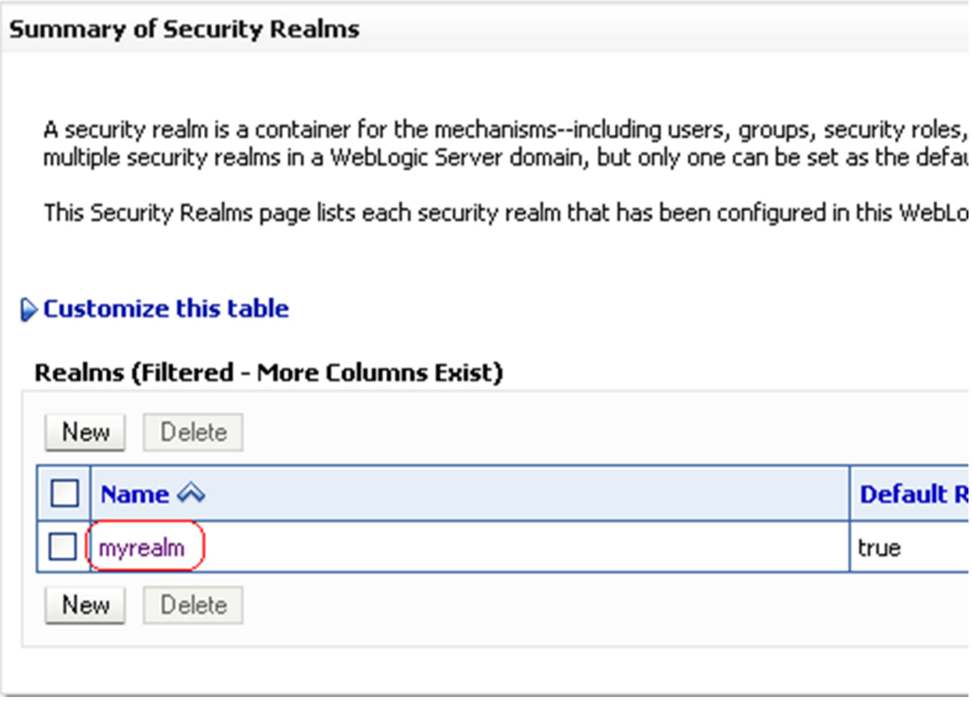
2. **Log in using the WebLogic Admin Console username and password you defined during STA installation.**

3. **Click Security Realms.**



ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Home
Change Center
View changes and restarts
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.
Domain Structure
DefaultDomain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
Home Page
Information and Resources
Helpful Tools
Configure applications
Recent Task Status
Set your console preferences
Domain Configurations
Domain
Domain
Environment
Servers
Clusters

4. **Click myrealm (select the name itself, you cannot check the box).**



Summary of Security Realms

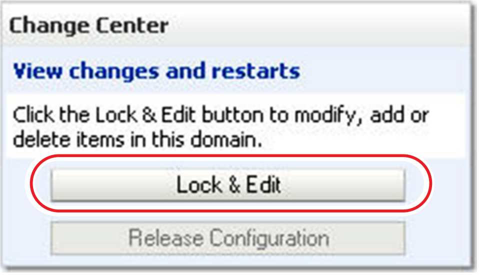
A security realm is a container for the mechanisms--including users, groups, security roles, multiple security realms in a WebLogic Server domain, but only one can be set as the defau

This Security Realms page lists each security realm that has been configured in this WebLo

Realms (Filtered - More Columns Exist)

| □ | Name | Default R |
|---|---|---|
| □ | myrealm | true |

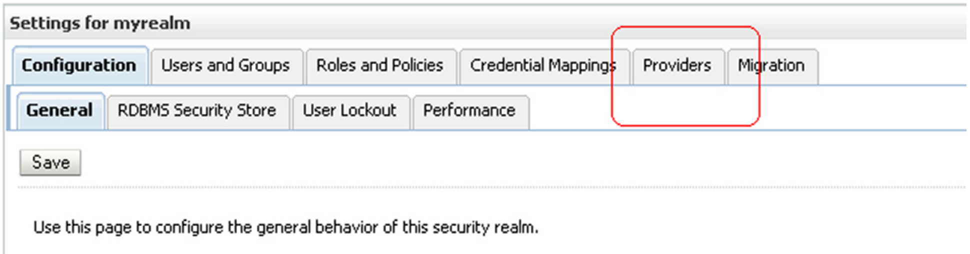
5. Click Lock & Edit.



Change Center

Click the Lock & Edit button to modify, add or delete items in this domain.

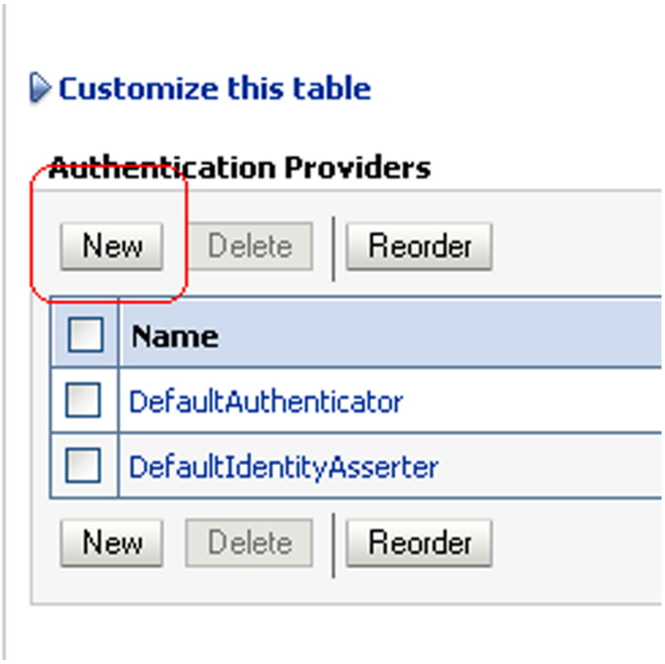
6. Select the Providers tab.



Settings for myrealm

Use this page to configure the general behavior of this security realm.

7. **Click New.**

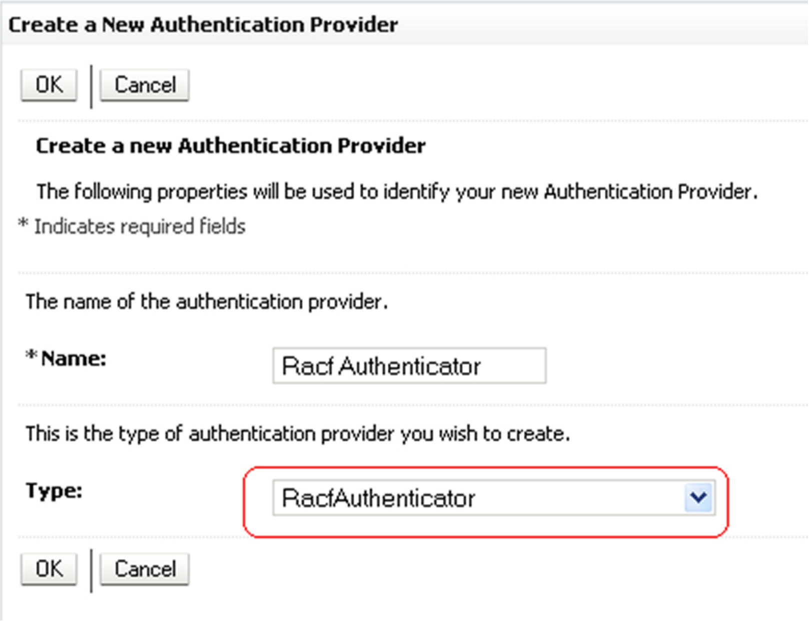


Authentication Providers

| □ | Name |
|---|---|
| □ | DefaultAuthenticator |
| □ | DefaultIdentityAsserter |

8. **Enter the name of the authentication provider and select RacfAuthenticator in the Type list. Click OK.**

   In the Type list, the RACF `jar` file should be listed. If it is not, stop and restart STA. See the "STA Command" section within the *StorageTek Tape Analytics Administration Reference Guide*.



**Create a New Authentication Provider**

**Create a new Authentication Provider**

The following properties will be used to identify your new Authentication Provider.

* Indicates required fields

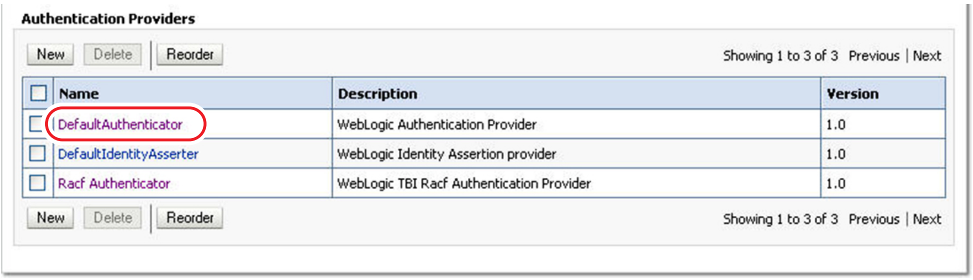
The name of the authentication provider.

***Name:** Racf Authenticator

This is the type of authentication provider you wish to create.

**Type:** RacfAuthenticator

Make sure the RACF provider is last in the list. The **DefaultAuthenticator** and **DefaultIdentityAsserter** must always be the first two items in this list.



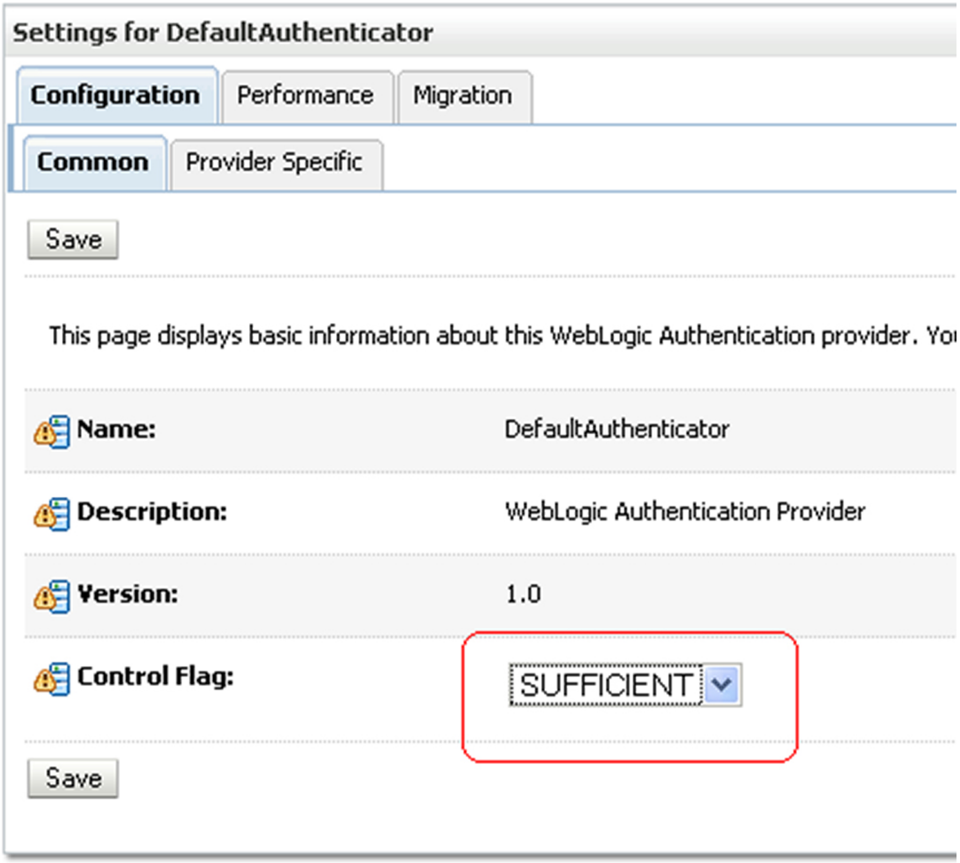
**Authentication Providers**

New
Delete
Reorder
Showing 1 to 3 of 3 Previous | Next

| ☐ | Name | Description | Version |
|---|---|---|---|
| ☐ | DefaultAuthenticator | WebLogic Authentication Provider | 1.0 |
| ☐ | DefaultIdentityAsserter | WebLogic Identity Assertion provider | 1.0 |
| ☐ | Racf Authenticator | WebLogic TBI Racf Authentication Provider | 1.0 |

New
Delete
Reorder
Showing 1 to 3 of 3 Previous | Next

9. **Click DefaultAthenticator (select the name itself, you cannot check the box).**
10. **Change the Control Flag to Sufficient and click Save.**



Settings for DefaultAuthenticator

This page displays basic information about this WebLogic Authentication provider. Yo

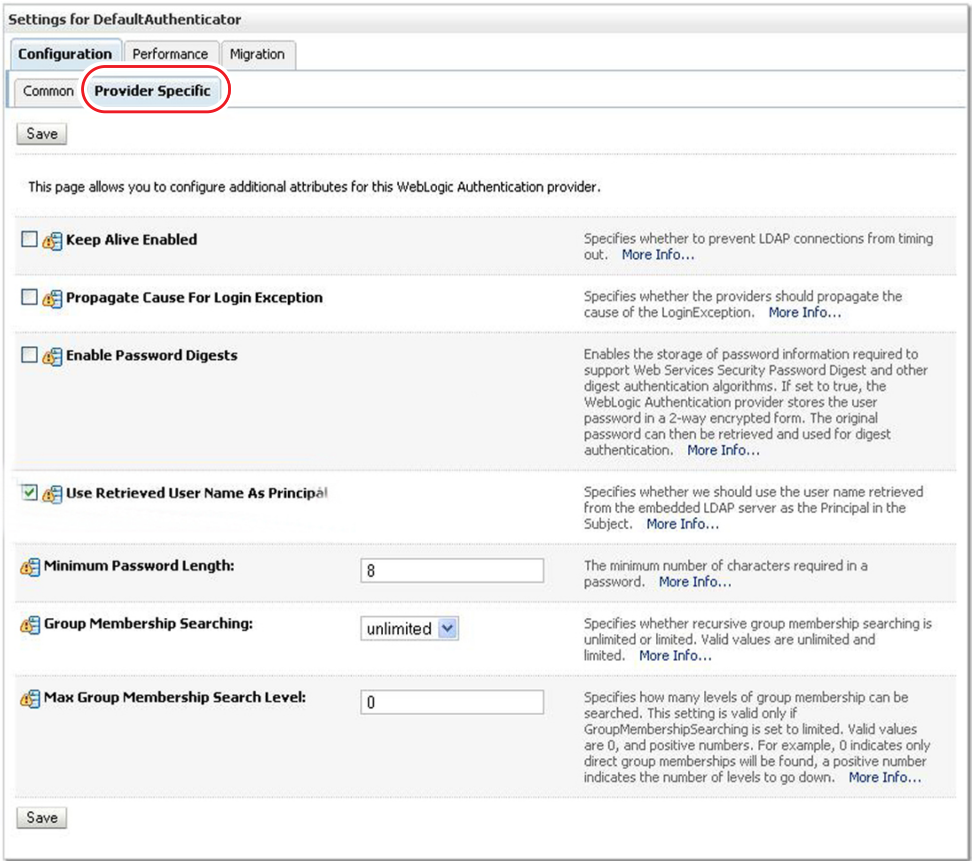
Name: DefaultAuthenticator

Description: WebLogic Authentication Provider

Version: 1.0

Control Flag: SUFFICIENT

11. Select the Provider Specific tab for the DefaultAuthenticator. Click Save.



Settings for DefaultAuthenticator

This page allows you to configure additional attributes for this WebLogic Authentication provider.

□ Keep Alive Enabled — Specifies whether to prevent LDAP connections from timing out. More Info...

□ Propagate Cause For Login Exception — Specifies whether the providers should propagate the cause of the LoginException. More Info...

□ Enable Password Digests — Enables the storage of password information required to support Web Services Security Password Digest and other digest authentication algorithms. If set to true, the WebLogic Authentication provider stores the user password in a 2-way encrypted form. The original password can then be retrieved and used for digest authentication. More Info...

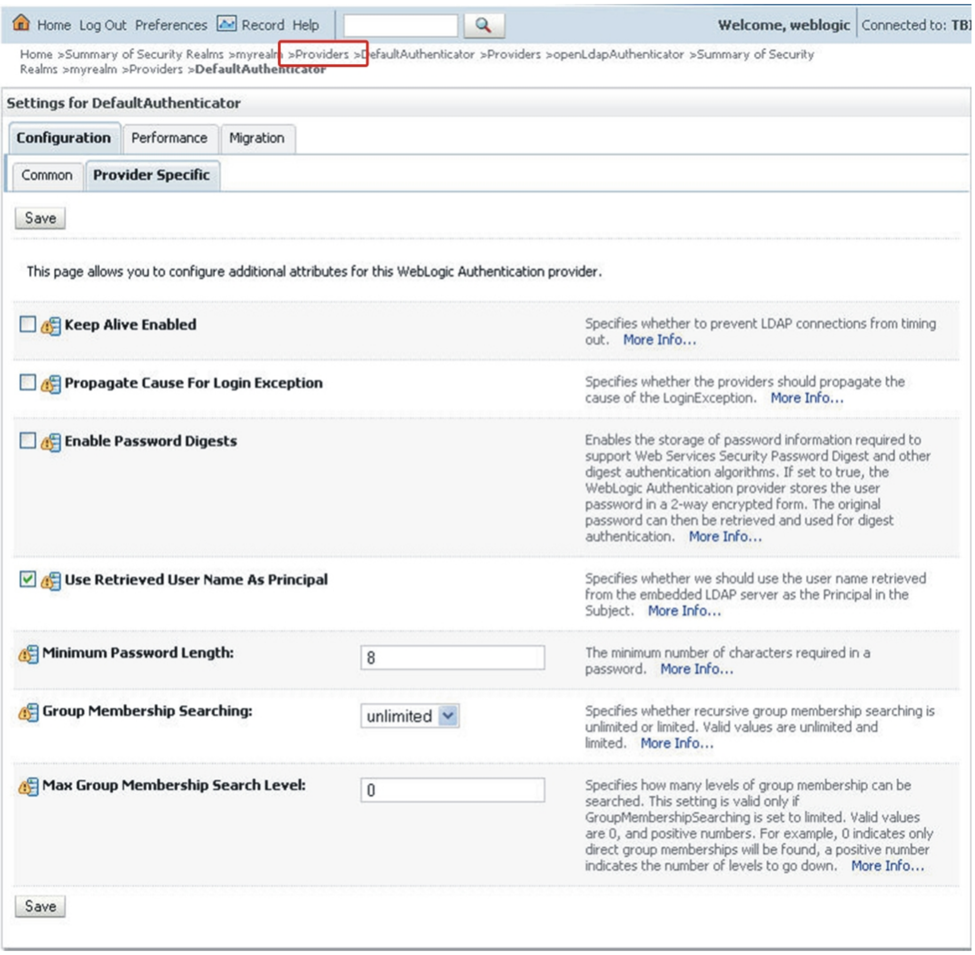
☑ Use Retrieved User Name As Principal — Specifies whether we should use the user name retrieved from the embedded LDAP server as the Principal in the Subject. More Info...

Minimum Password Length: 8 — The minimum number of characters required in a password. More Info...

Group Membership Searching: unlimited — Specifies whether recursive group membership searching is unlimited or limited. Valid values are unlimited and limited. More Info...

Max Group Membership Search Level: 0 — Specifies how many levels of group membership can be searched. This setting is valid only if GroupMembershipSearching is set to limited. Valid values are 0, and positive numbers. For example, 0 indicates only direct group memberships will be found, a positive number indicates the number of levels to go down. More Info...

**12. Click the Providers link to return to the Providers -> Authentication screen.**



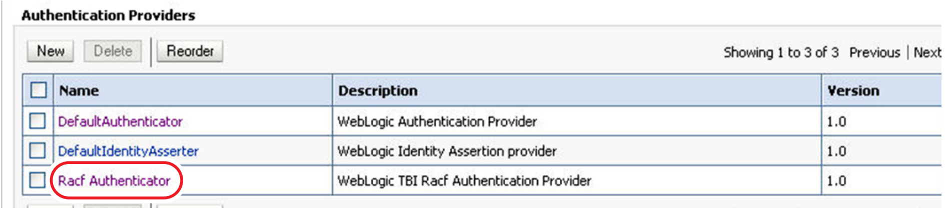
Home >Summary of Security Realms >myrealm >Providers >DefaultAuthenticator >Providers >openLdapAuthenticator >Summary of Security Realms >myrealm >Providers >**DefaultAuthenticator**

**Settings for DefaultAuthenticator**

This page allows you to configure additional attributes for this WebLogic Authentication provider.

| | | |
|---|---|---|
| □ **Keep Alive Enabled** | | Specifies whether to prevent LDAP connections from timing out. More Info... |
| □ **Propagate Cause For Login Exception** | | Specifies whether the providers should propagate the cause of the LoginException. More Info... |
| □ **Enable Password Digests** | | Enables the storage of password information required to support Web Services Security Password Digest and other digest authentication algorithms. If set to true, the WebLogic Authentication provider stores the user password in a 2-way encrypted form. The original password can then be retrieved and used for digest authentication. More Info... |
| ☑ **Use Retrieved User Name As Principal** | | Specifies whether we should use the user name retrieved from the embedded LDAP server as the Principal in the Subject. More Info... |
| **Minimum Password Length:** | 8 | The minimum number of characters required in a password. More Info... |
| **Group Membership Searching:** | unlimited | Specifies whether recursive group membership searching is unlimited or limited. Valid values are unlimited and limited. More Info... |
| **Max Group Membership Search Level:** | 0 | Specifies how many levels of group membership can be searched. This setting is valid only if GroupMembershipSearching is set to limited. Valid values are 0, and positive numbers. For example, 0 indicates only direct group memberships will be found, a positive number indicates the number of levels to go down. More Info... |

13. Click RacfAthenticator (select the name itself, you cannot check the box).

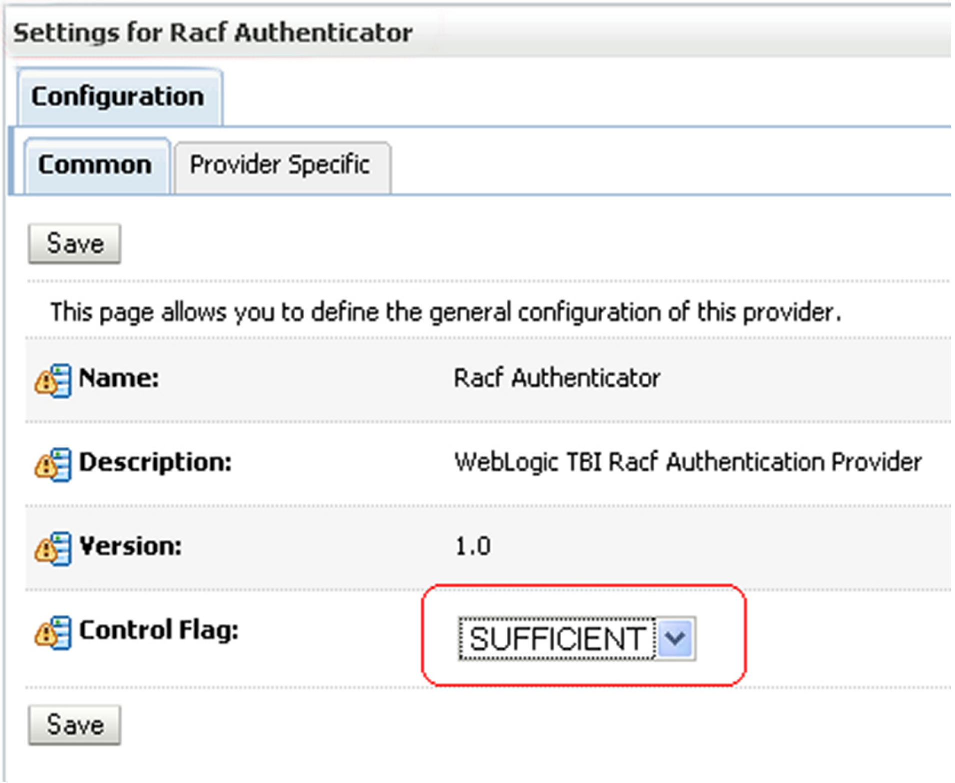


**Authentication Providers**

Showing 1 to 3 of 3 Previous | Next

| □ | Name | Description | Version |
|---|---|---|---|
| □ | DefaultAuthenticator | WebLogic Authentication Provider | 1.0 |
| □ | DefaultIdentityAsserter | WebLogic Identity Assertion provider | 1.0 |
| □ | Racf Authenticator | WebLogic TBI Racf Authentication Provider | 1.0 |

14. Change the Control Flag to Sufficient and click Save.

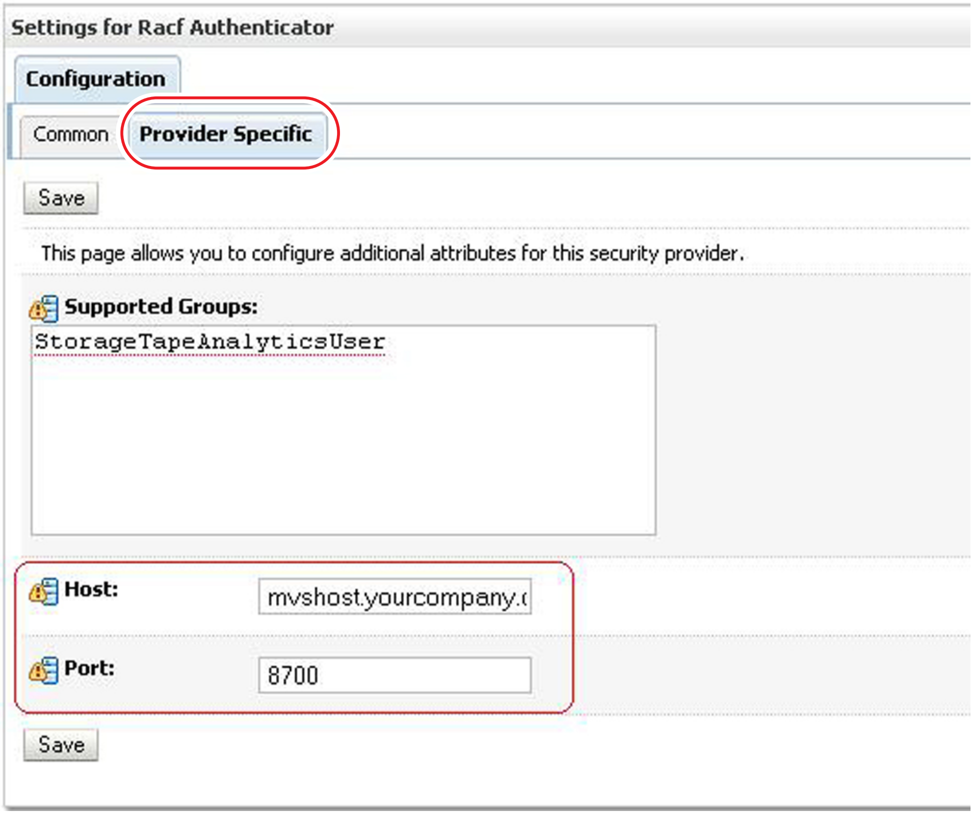


Settings for Racf Authenticator

This page allows you to define the general configuration of this provider.

| | |
|---|---|
| Name: | Racf Authenticator |
| Description: | WebLogic TBI Racf Authentication Provider |
| Version: | 1.0 |
| Control Flag: | SUFFICIENT |

15. Select the Provider Specific tab for the RacfAuthenticator. Enter the host name and port number where the MVS system is running. Click Save.



Settings for Racf Authenticator

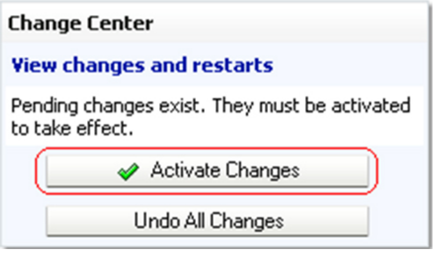
This page allows you to configure additional attributes for this security provider.

Supported Groups: StorageTapeAnalyticsUser

Host: mvshost.yourcompany.c

Port: 8700

16. Click Activate Changes.



Change Center

Pending changes exist. They must be activated to take effect.

17. Log out of WebLogic.

18. From the Linux command line, stop and restart STA.

```
# STA stop
Stopping the WebLogic staServer....
Successfully stopped the WebLogic staServer
Stopping the WebLogic Administration Server....
Successfully stopped the WebLogic Administration Server
Stopping the STA Database Server Backup Service (staservd)....
Successfully stopped the STA Database Server Backup Service
Stopping the STA database Server....
Successfully stopped the STA Database Server
```

```
# STA start
Starting STA Database....
Successfully started the STA Database
Starting STA Database Backup Service (staservd)....
Successfully started the STA Database Backup Service
Starting WebLogic Administration Server....
Successfully started the WebLogic Administration Server
Starting WebLogic staServer....
Successfully started the WebLogic staServer
```

# 7

# Configuring Certificates

This chapter discusses information about setting up an HTTPS/SSL connection and replacing the certificate Oracle provides you with one you choose.

This chapter discusses the following topics:

- "Oracle Certificate" on page 181
- "Establishing the Initial HTTPS/SSL Connection" on page 182
- "Reconfigure the WebLogic Server to use a Different Security Certificate" on page 187
- "Replace the Oracle Certificate" on page 194.

## Oracle Certificate

Oracle supplies self-generated certificates to be used with HTTPS/SSL Ports. During installation, STA generates a certificate using the Java keytool and creates it on your server, using your server hostname.

This way, you can be sure the certificate is coming from the proper server and when you view it, you can verify the hostname along with the Oracle information.

If you wish, you can replace the Oracle certificate with your own approved certificate from a selected certificate authority (for example, VeriSign).

You must perform the following procedures to accept and connect to STA using an HTTPS/SSL connection and, optionally, to replace the Oracle certificate if you elect to.

- "Establishing the Initial HTTPS/SSL Connection" on page 182
- "Reconfigure the WebLogic Server to use a Different Security Certificate" on page 187.

After you complete these tasks, you must define the keystore and SSL private key alias settings in WebLogic.

- "Reconfigure the WebLogic Server to use a Different Security Certificate" on page 187.

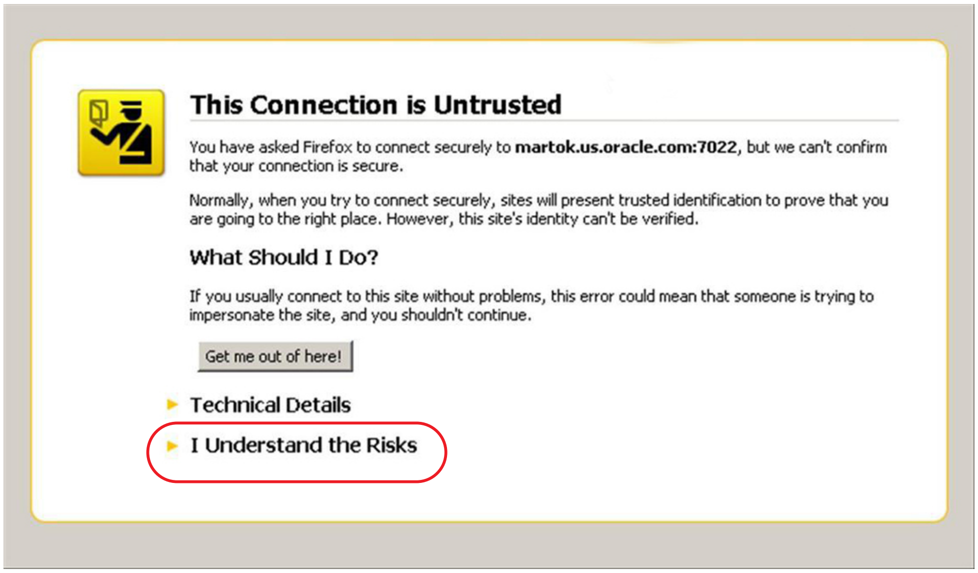
## ▼ Establishing the Initial HTTPS/SSL Connection

The procedure shown here uses Mozilla Firefox running on a Windows platform. Steps may differ on other browsers and operating system platforms.

1. **Enter the HTTPS/SSL version of the URL for the STA application on the browser.**

https://*your_localhost.com:port number*/STA/

2. **Click I Understand the Risks on the This Connection is Untrusted screen.**



**This Connection is Untrusted**

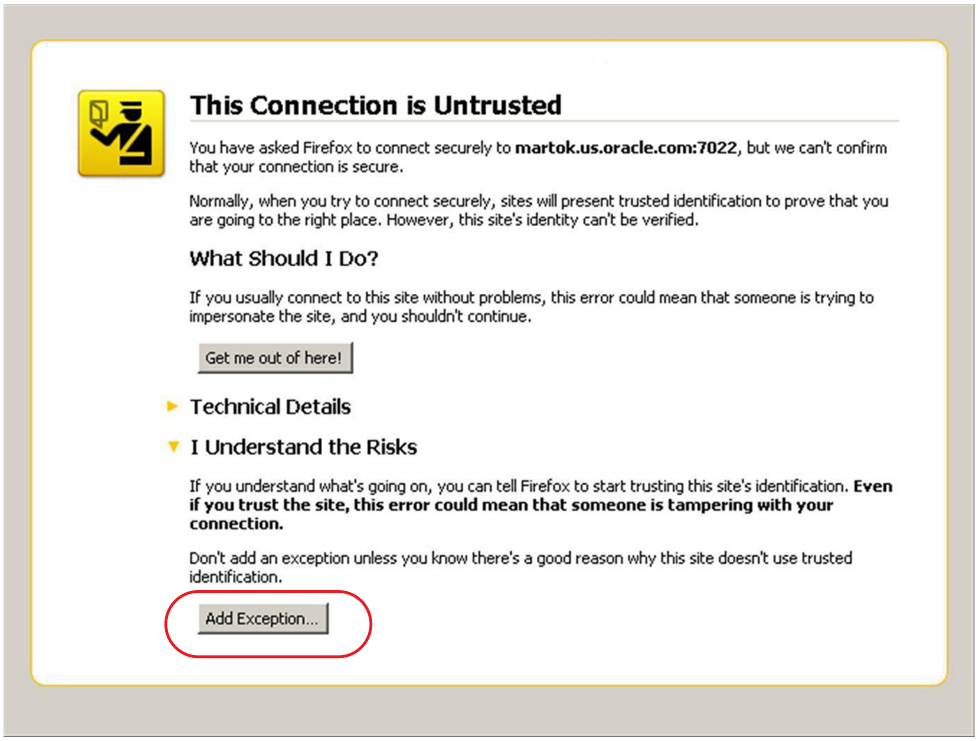
You have asked Firefox to connect securely to **martok.us.oracle.com:7022**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

**What Should I Do?**

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

3. **Click Add Exception.**



This Connection is Untrusted

You have asked Firefox to connect securely to **martok.us.oracle.com:7022**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

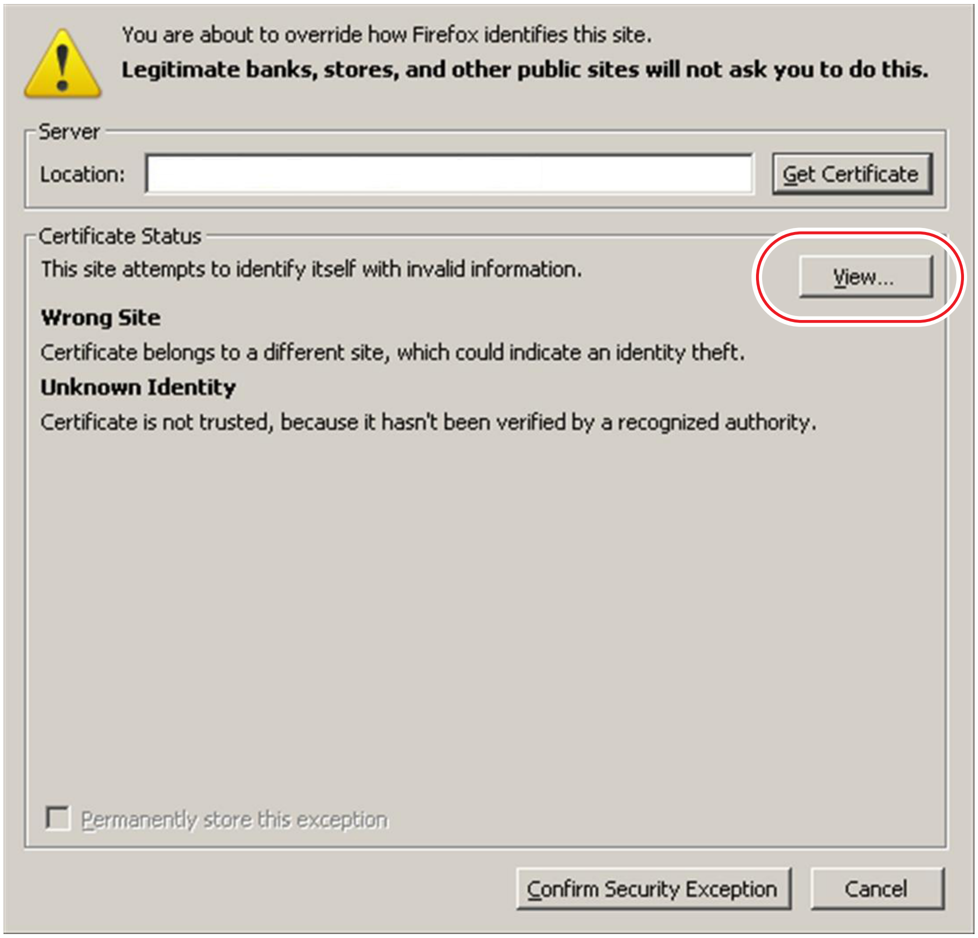
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

**4. Click View on the Add Security Certificate screen to see the Oracle certificate.**



You are about to override how Firefox identifies this site.

**Legitimate banks, stores, and other public sites will not ask you to do this.**

This site attempts to identify itself with invalid information.

**Wrong Site**

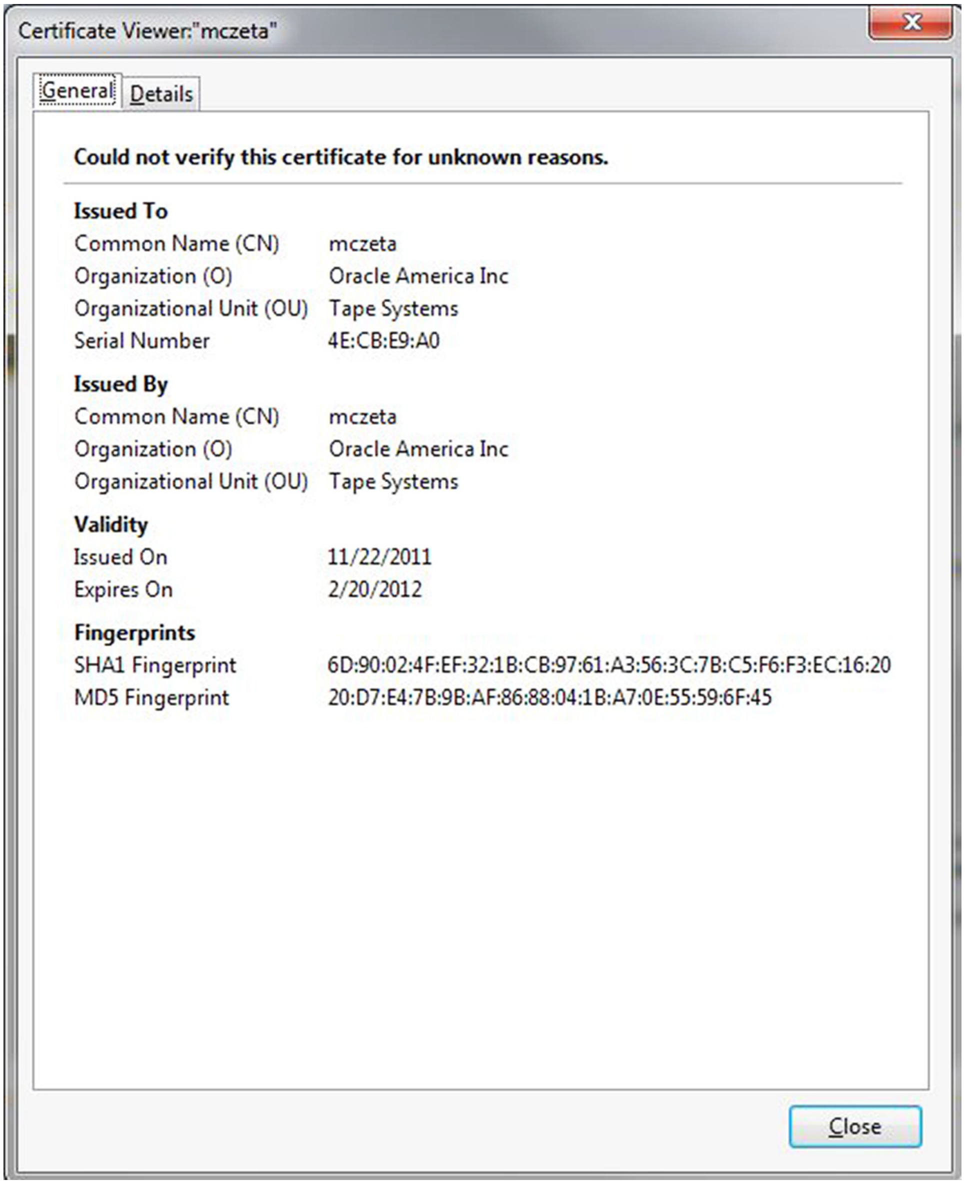
Certificate belongs to a different site, which could indicate an identity theft.

**Unknown Identity**

Certificate is not trusted, because it hasn't been verified by a recognized authority.

□ Permanently store this exception
Confirm Security Exception
Cancel

You then see the Certificate Viewer: *your_localhost* screen. The certificate is not shown as verified because it is not from a certificate authority.



**Could not verify this certificate for unknown reasons.**

**Issued To**

| | |
|---|---|
| Common Name (CN) | mczeta |
| Organization (O) | Oracle America Inc |
| Organizational Unit (OU) | Tape Systems |
| Serial Number | 4E:CB:E9:A0 |

**Issued By**

| | |
|---|---|
| Common Name (CN) | mczeta |
| Organization (O) | Oracle America Inc |
| Organizational Unit (OU) | Tape Systems |

**Validity**

| | |
|---|---|
| Issued On | 11/22/2011 |
| Expires On | 2/20/2012 |

**Fingerprints**

| | |
|---|---|
| SHA1 Fingerprint | 6D:90:02:4F:EF:32:1B:CB:97:61:A3:56:3C:7B:C5:F6:F3:EC:16:20 |
| MD5 Fingerprint | 20:D7:E4:7B:9B:AF:86:88:04:1B:A7:0E:55:59:6F:45 |

You can examine the certificate further on the **Certificate Viewer** screen by clicking the **Details** tab and selecting the **issuer** field. The variables you may see include:

- CN = The hostname of the server that the STA application has been installed on. For example,

```
Common Name (CN) your server name
```

- OU = Tape Systems
- O = Oracle America Inc
- L = Redwood City

- ST = California
- C = USA

The variable field CN is the server name that the certificate was generated on.

5. **Click Close to return to the Add Security Certificate screen.**
6. **Click  Confirm Security Exception on the Add Security Certificate screen, and you will be able to use HTTPS with the proper certificate.**

You return to the URL you entered in Step 1.

## ▼ Reconfigure the WebLogic Server to use a Different Security Certificate

**Caution –** You must remember the WebLogic administration account usernames and passwords you establish in this procedure. If you forget the usernames or passwords, you must re-install STA.

1. **Point your browser to the WebLogic console login screen.**

   http://*yourHostName*:7001/console/

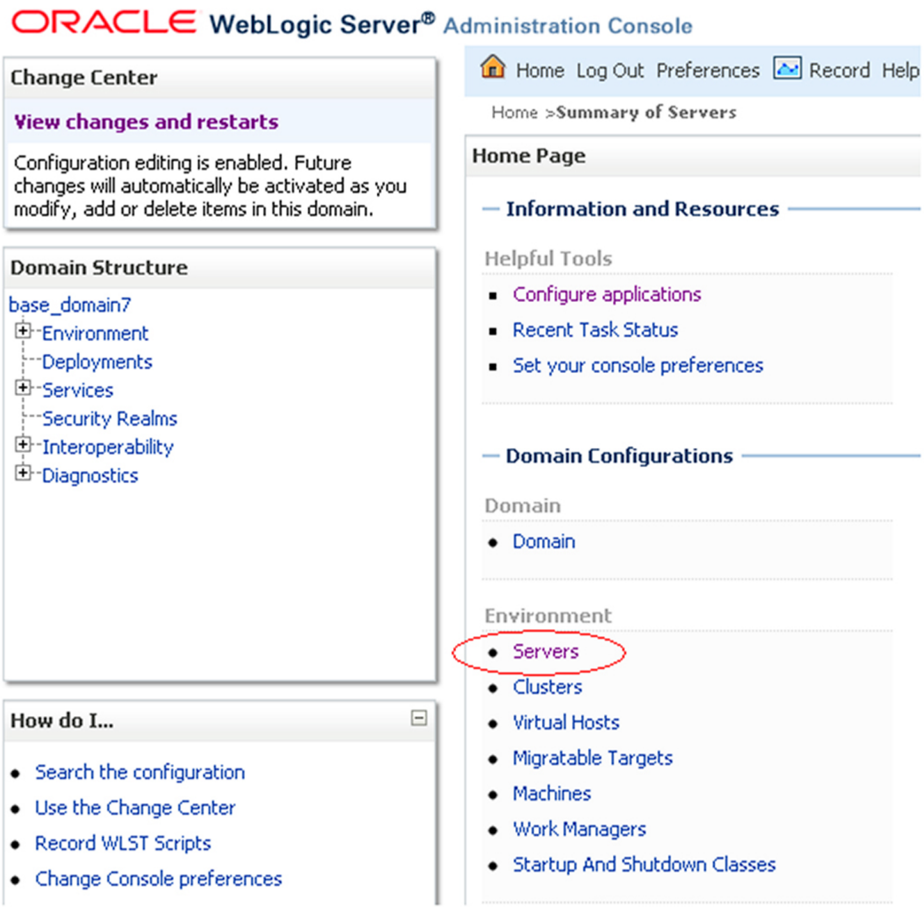
   or

   https://*yourHostName*:7002/console/

   **Note –** Use the HTTP or HTTPS port number you selected during STA installation.

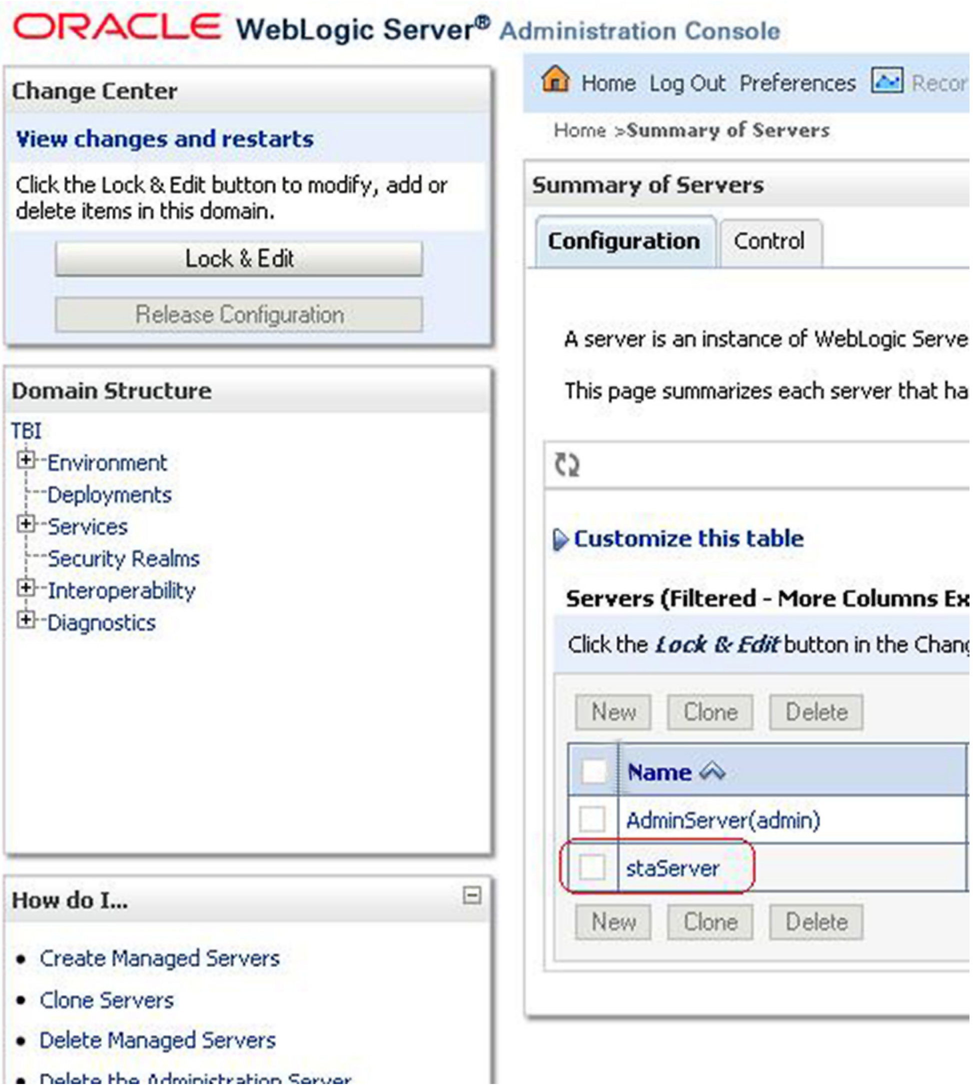
2. **Log in using the WebLogic Admin Console username and password you defined during STA installation.**

3. **On the home page, select Servers.**



Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

4. **On the Summary of Servers page, select staServer.**



Click the Lock & Edit button to modify, add or delete items in this domain.

A server is an instance of WebLogic Serve

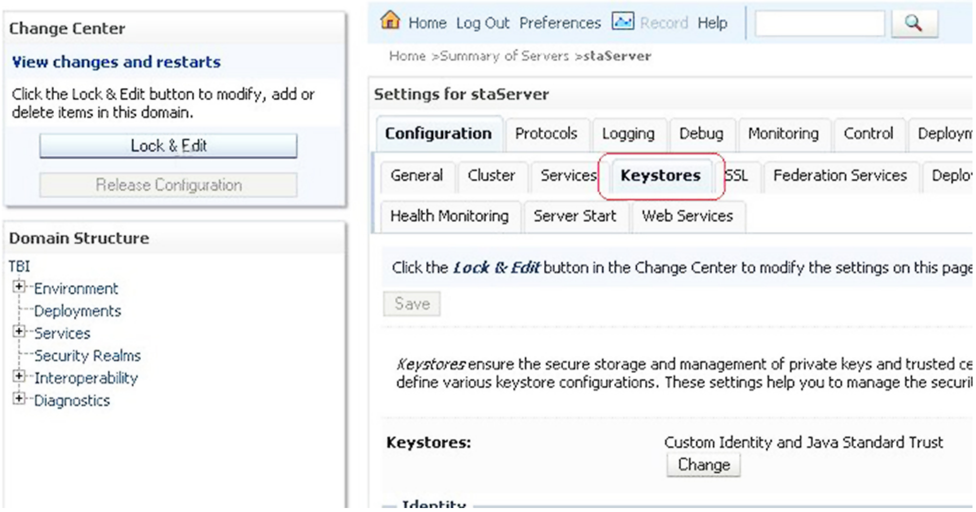
This page summarizes each server that ha

Servers (Filtered - More Columns Ex

Click the *Lock & Edit* button in the Chang

| □ | Name |
|---|---|
| □ | AdminServer(admin) |
| □ | staServer |

5. **On the Settings for staServer screen, click the Keystores tab.**



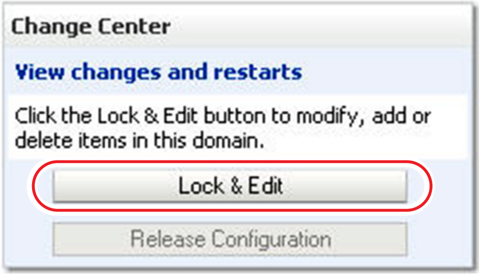
Click the Lock & Edit button to modify, add or delete items in this domain.

Click the *Lock & Edit* button in the Change Center to modify the settings on this page

*Keystores* ensure the secure storage and management of private keys and trusted ce define various keystore configurations. These settings help you to manage the securi

Keystores: Custom Identity and Java Standard Trust

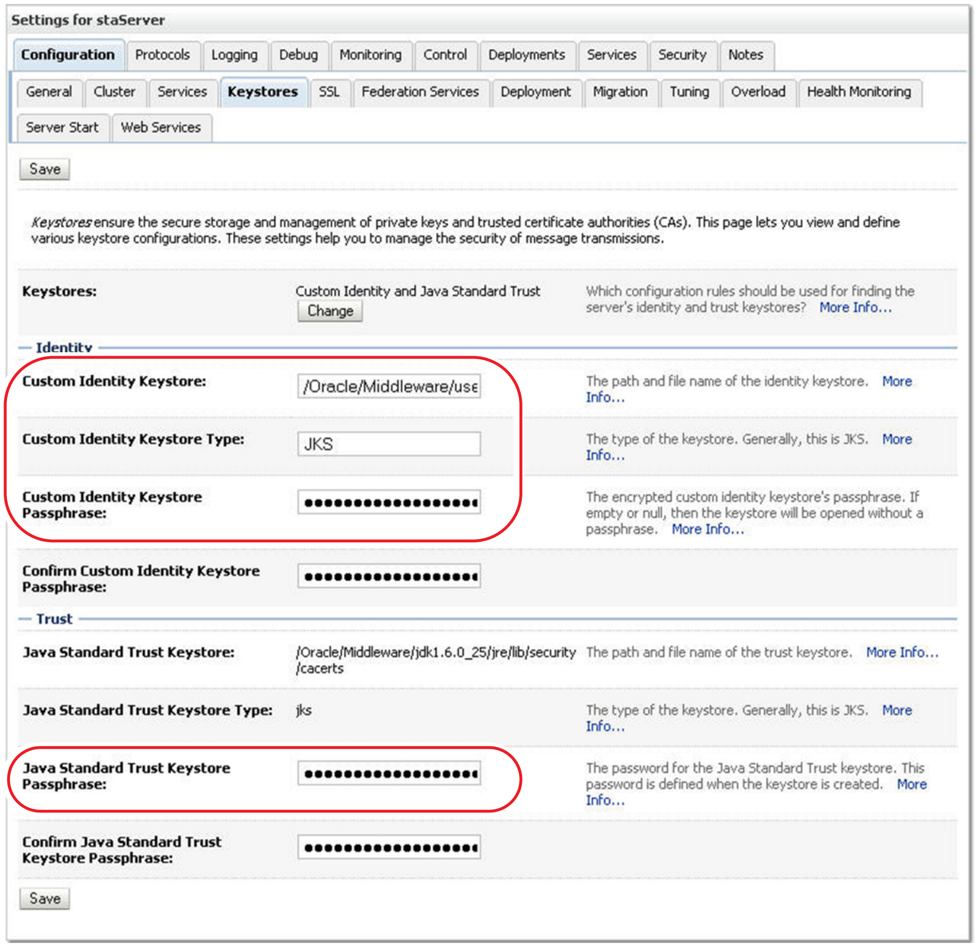
6. Click Lock & Edit.



Click the Lock & Edit button to modify, add or delete items in this domain.

7. On the Keystores screen, enter:
   a. the path and file of the private key file
   b. the Keystore Type
   c. the password supplied by the MVS system administrator
   d. the new password for the Java Standard Trust Keystore file (do not enter changeit).

   **Caution –** You must remember the WebLogic administration account usernames and passwords you enter. If you forget the usernames or passwords, you must re-install STA.



*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...

**Identity**

**Custom Identity Keystore:** /Oracle/Middleware/use — The path and file name of the identity keystore. More Info...

**Custom Identity Keystore Type:** JKS — 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:** /Oracle/Middleware/jdk1.6.0_25/jre/lib/security /cacerts — The path and file name of the trust keystore. More Info...

**Java Standard Trust Keystore Type:** jks — The type of the keystore. Generally, this is JKS. More Info...

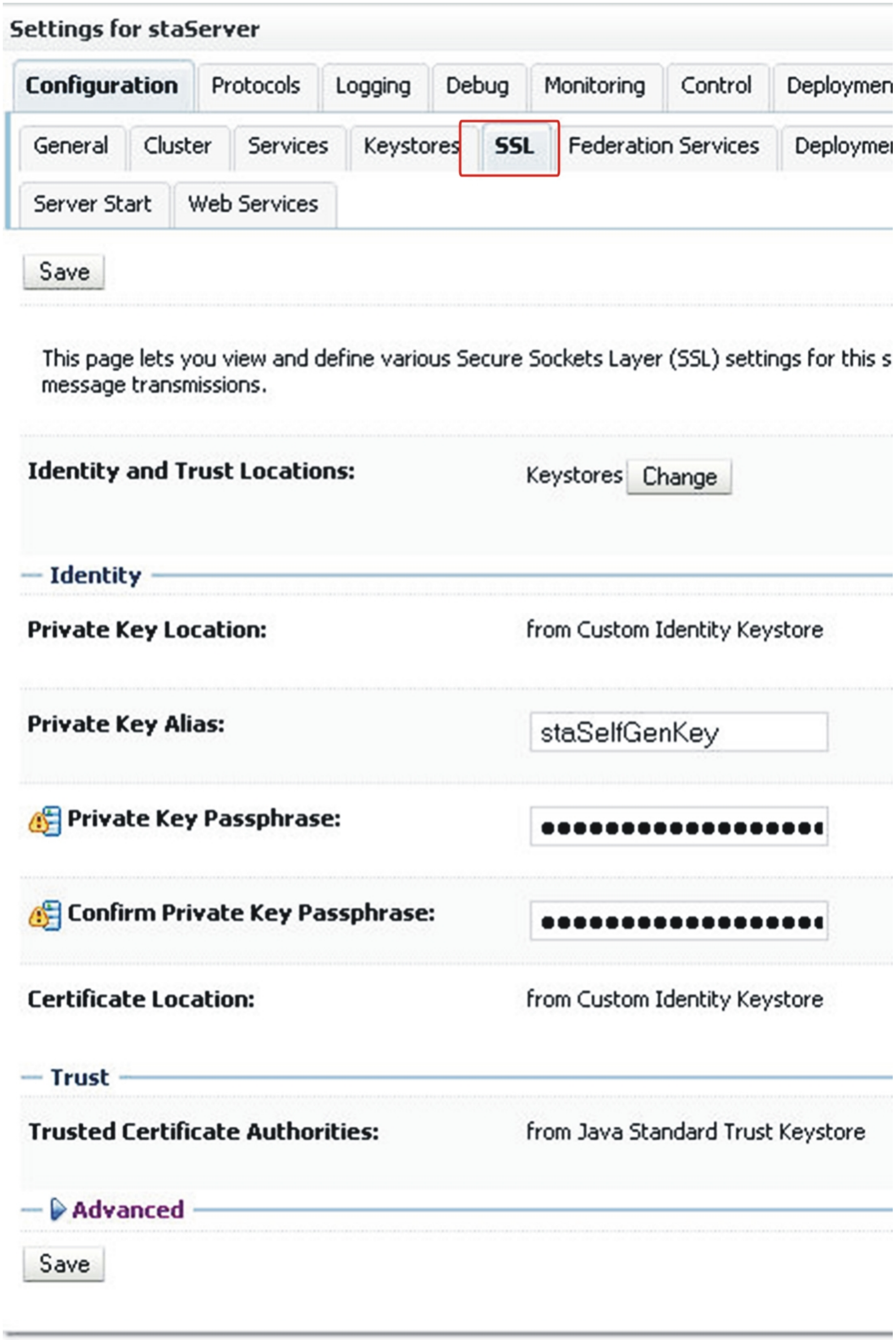
**Java Standard Trust Keystore Passphrase:** ••••••••••••••••••• — The password for the Java Standard Trust keystore. This password is defined when the keystore is created. More Info...

**Confirm Java Standard Trust Keystore Passphrase:** •••••••••••••••••••

8. **Click Save.**
9. **Click the SSL secondary tab, enter the Private Key Alias and the password supplied by the MVS system programmer.**

   To determine the Private Key Alias, use the **keytool** command. For example:

```
C:\Temp>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
```



Settings for staServer

This page lets you view and define various Secure Sockets Layer (SSL) settings for this s message transmissions.

Identity and Trust Locations: Keystores

Private Key Location: from Custom Identity Keystore

Private Key Alias: staSelfGenKey

Private Key Passphrase: ●●●●●●●●●●●●●●●●●●

Confirm Private Key Passphrase: ●●●●●●●●●●●●●●●●●●

Certificate Location: from Custom Identity Keystore

Trusted Certificate Authorities: from Java Standard Trust Keystore

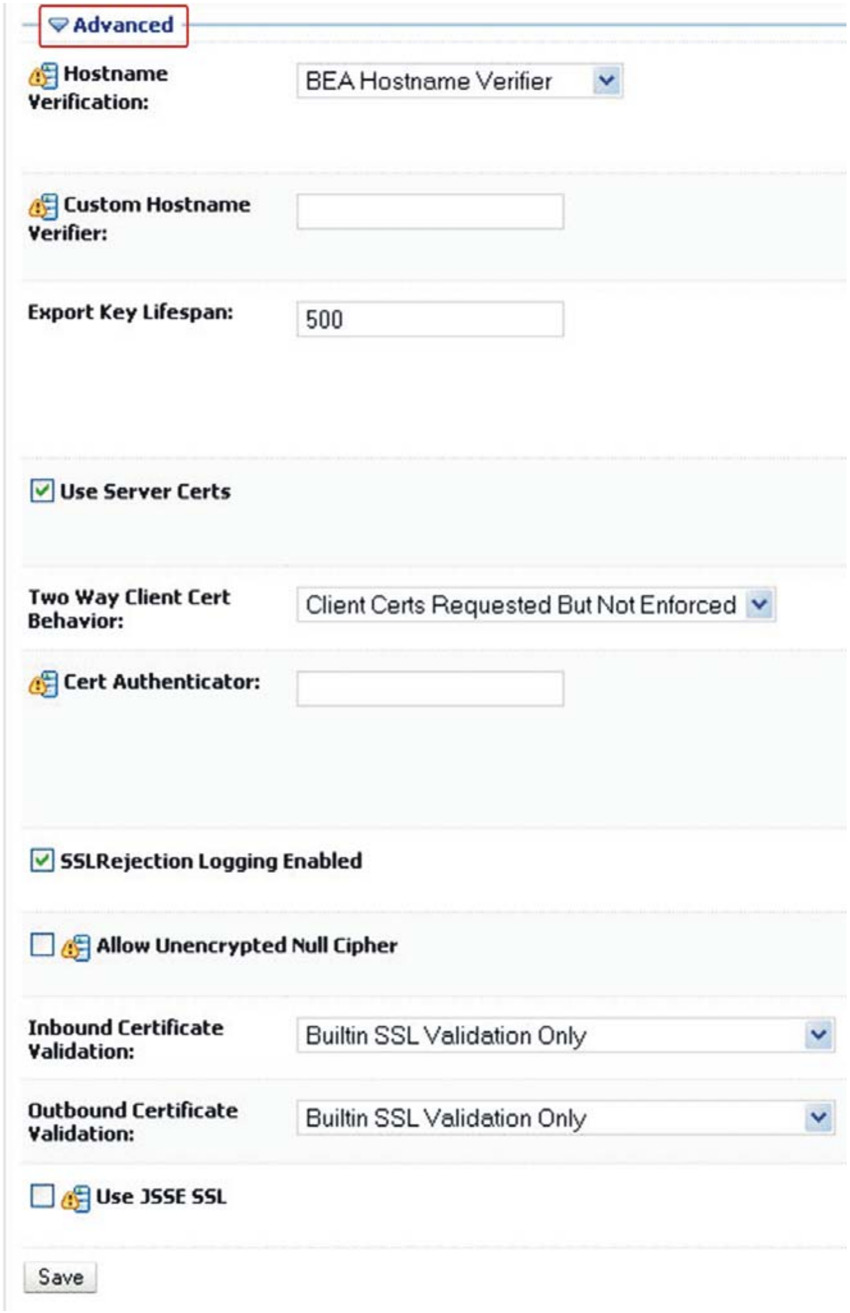
10. Select the Advanced link.

11. Modify the following information:

a. **Select the Use Server Certs check box.**

b. **From the Two Way Client Cert Behavior list, select Client Certs Requested and Enforced.**

c. **Select Builtin SSL Validation and Cert Path Validators from both the Inbound Certification Validation and Outbound Certificate Validation lists.**



Hostname Verification: BEA Hostname Verifier

Custom Hostname Verifier:

Export Key Lifespan: 500

☑ Use Server Certs

Two Way Client Cert Behavior: Client Certs Requested But Not Enforced

Cert Authenticator:

☑ SSLRejection Logging Enabled

□ Allow Unencrypted Null Cipher

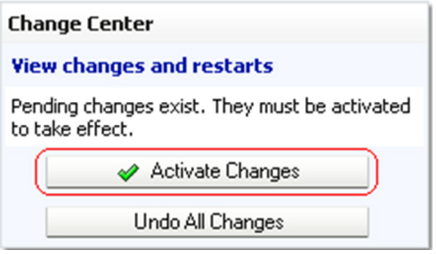
Inbound Certificate Validation: Builtin SSL Validation Only

Outbound Certificate Validation: Builtin SSL Validation Only

□ Use JSSE SSL

12. **Click Save.**

**13. Click Activate Changes.**



Change Center

View changes and restarts

Pending changes exist. They must be activated to take effect.

**14. Stop and restart STA.**

```
# STA stop
Stopping the WebLogic staServer....
Successfully stopped the WebLogic staServer
Stopping the WebLogic Administration Server....
Successfully stopped the WebLogic Administration Server
Stopping the STA Database Server Backup Service (staservd)....
Successfully stopped the STA Database Server Backup Service
Stopping the STA database Server....
Successfully stopped the STA Database Server

# STA start
Starting STA Database....
Successfully started the STA Database
Starting STA Database Backup Service (staservd)....
Successfully started the STA Database Backup Service
Starting WebLogic Administration Server....
Successfully started the WebLogic Administration Server
Starting WebLogic staServer....
Successfully started the WebLogic staServer
```

**15. Log in using your username and password.**

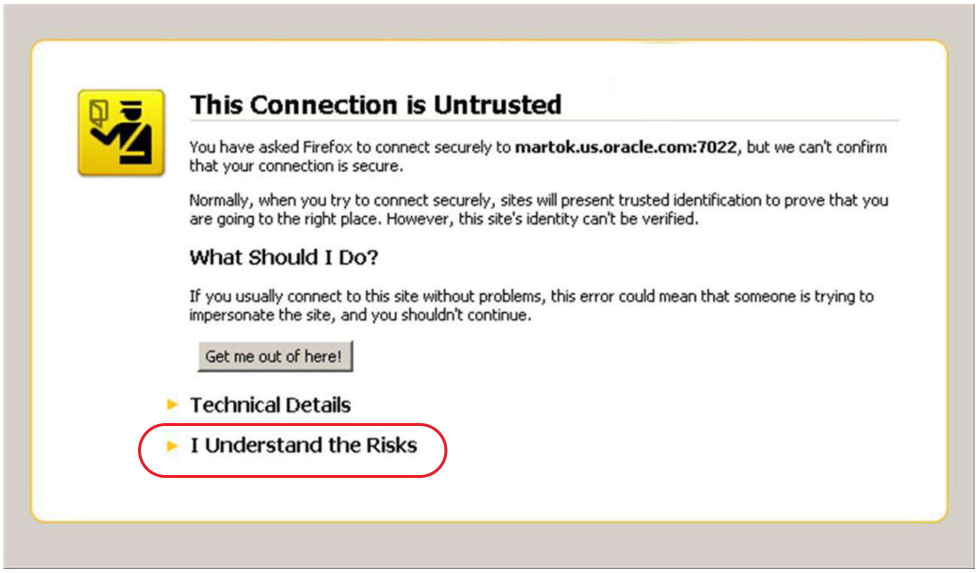
## ▼ Replace the Oracle Certificate

The procedure shown here uses Mozilla Firefox running on a Windows platform. Steps may differ on other browsers and operating system platforms.

1. **Enter the HTTPS/SSL version of the URL for the STA application on the browser.**

https://*your_localhost.com:port number*/STA/

2. **Select I Understand the Risks on the This Connection is Untrusted screen.**



This Connection is Untrusted

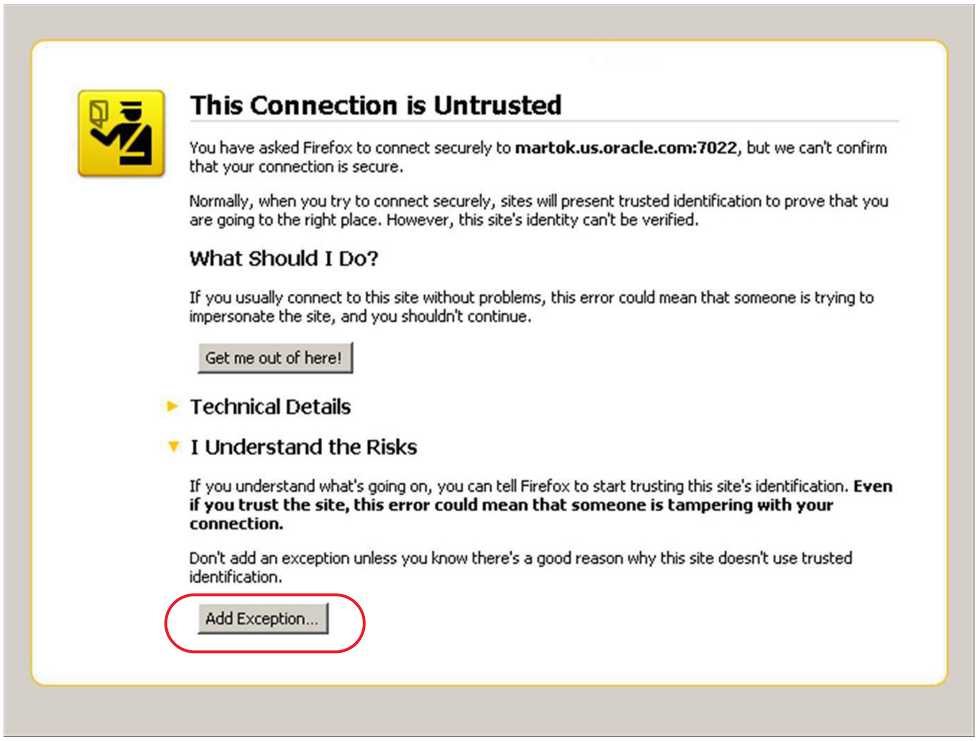
You have asked Firefox to connect securely to **martok.us.oracle.com:7022**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

3. **Click Add Exception.**



This Connection is Untrusted

You have asked Firefox to connect securely to **martok.us.oracle.com:7022**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

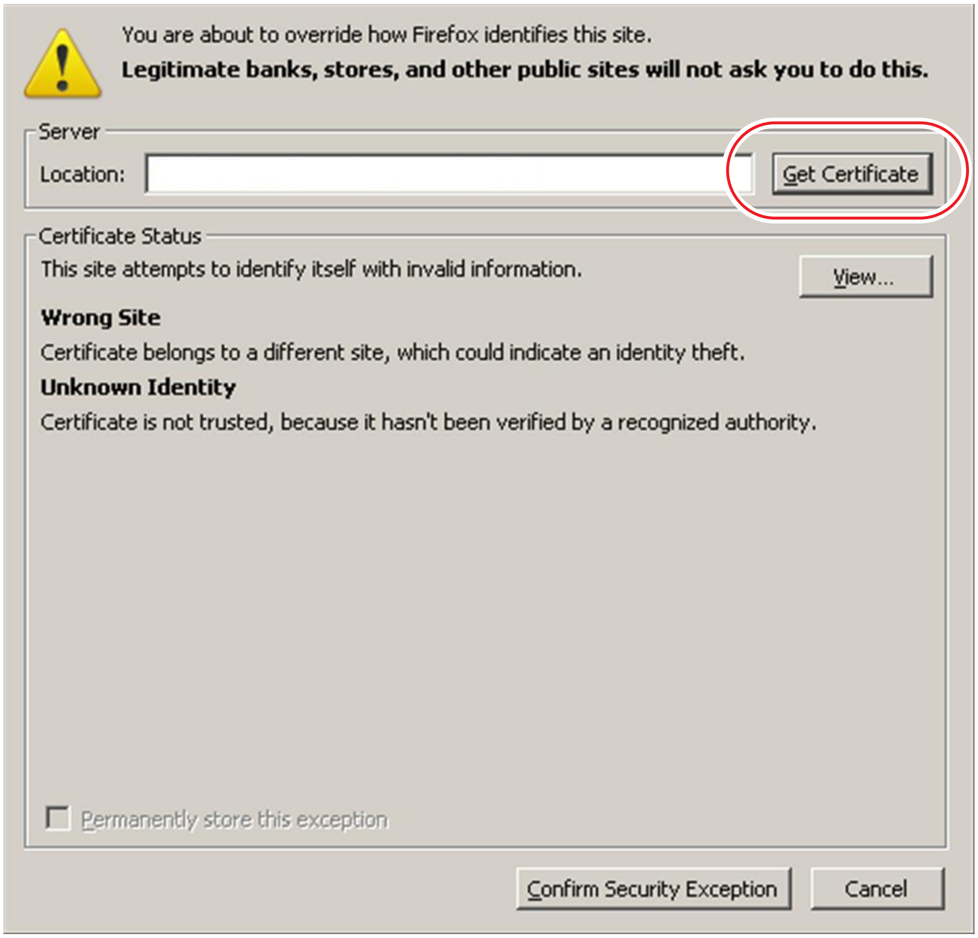
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

4. **To specify a certificate for your organization, click Get Certificate on the Add Security Certificate screen and select the appropriate file.**



You are about to override how Firefox identifies this site.

**Legitimate banks, stores, and other public sites will not ask you to do this.**

Server

Location:

Certificate Status

This site attempts to identify itself with invalid information.

**Wrong Site**

Certificate belongs to a different site, which could indicate an identity theft.

**Unknown Identity**

Certificate is not trusted, because it hasn't been verified by a recognized authority.

□ Permanently store this exception

5. **Click Confirm Security Exception.**

You return to the URL you entered in Step 1.

# A

# Configuring SNMP v2c Mode

> **Note –** The information in this appendix applies only if you have elected to use SNMP v2c for SNMP communications between STA and the libraries.

SNMP v3 is the recommended protocol for SNMP communications between STA and the libraries. Depending on your site requirements, however, you may choose to use v2c. See "SNMP Configuration for STA" on page 17 for details.

You will need to enable v2c mode if either of the following is true for your library environment:

- You want STA to monitor libraries configured for v2c.
- You want STA to monitor a mix of libraries configured for v3 and libraries configured for v2c.

> **Note –** STA always attempts to communicate with libraries with v3; however, if v3 communication is not possible (for instance, if v3 is not configured on the library), STA will use v2c if enabled as per this appendix.

The complete SNMP v3 configuration process is described in Chapter 1, Configuring the Libraries for STA" and Chapter 2, Configuring SNMP in the STA Application". This appendix describes *only* the specific procedures that differ for v2c configuration.

## SNMP v2c Mode Configuration Process

Use the following process to configure STA and the libraries to use SNMP v2c for SNMP communications.

1. In Chapter 1, follow all procedures shown in TABLE 1-4 on page 26, but with the following exceptions:
   - Replace "Create an SNMP v3 Trap Recipient" with "Create an SNMP v2c Trap Recipient" (in this appendix).
   - At the end of the process shown in TABLE 1-4, follow the procedure in "Enable SNMP v2c Mode for STA" on page 203 (in this appendix).
2. Follow the procedures in "Configuration Process" on page 75 (in Chapter 2).

# ▼ Create an SNMP v2c Trap Recipient

Use this procedure to define the STA server as an authorized recipient of SNMP v2c traps, and to define the traps that the library will send.

> **Note –** Before performing this procedure, you must obtain the IP address of the STA server, which was established during the STA installation. For details, see the “Installing STA” chapter within the *StorageTek Tape Analytics Planning and Installation Guide*.

> **Note –** If you want 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.

> **Note –** For SL500 libraries, you can choose to perform this procedure with either the CLI or the SL Console. For SL3000 and SL8500 libraries, you must use the CLI. For SL150 libraries, you use the browser-based user interface.

## ▼ With the CLI (All libraries except SL150)

1. **Use the following command to create a v2c SNMP trap recipient:**

> **Note –** Because of the complexity of this command, it is recommended that you create it in a text file on your PC or workstation, and then copy and paste the command directly into the CLI command line. See “CLI Usage Tips” on page 15 for details.

> **Note –** For SL3000 and SL8500 libraries, do not include trap level 4. It is not supported by the SL3000 and SL8500 libraries.

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

> **Note –** Trap levels must be entered individually, separated by commas (**,**).

Where:

- *STA_server_IP* is the IP address of the STA server.
- *community_name* is the v2c trap community. This can be **public**, or another name of your choice.

### *SL3000 Example*

> **Note –** The SL8500 display is similar.

```
SL3000> snmp addTrapRecipient trapLevel
1,2,3,11,21,25,27,41,45,61,63,65,81,85,100 host 10.80.125.23
version v2c community public
   requestId
   requestId 12345
   Device 1,0,0,0,0
   Success true
   Done
   Failure Count 0
   Success Count 1
COMPLETED
```

### *SL500 Example*

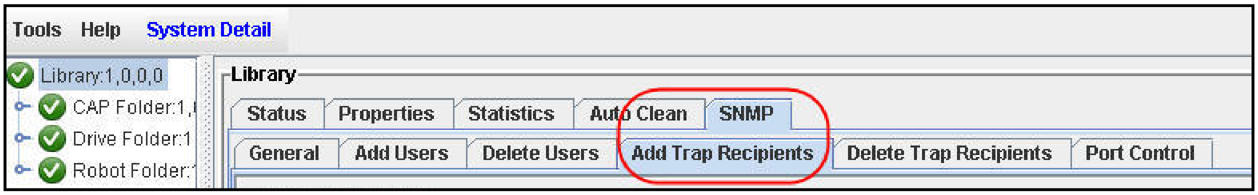
```
SL500> snmp addTrapRecipient trapLevel
1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100 host
10.80.125.23 version v2c community public
   requestId
   requestId 12345
   Device 1,0,0,0
   Success true
   Done
   Failure Count 0
   Success Count 1
COMPLETED
```

2. **List the trap recipients, and verify that this one has been added correctly.**

```
SL500> snmp listTrapRecipients
  requestId
  requestId 12345
  Attributes Community  public
             Host       10.80.125.23
             Index      1
             Port       162
             Trap Level 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100
             Version    v2c
   Object    Snmp       snmp
   Done
   Failure Count 0
   Success Count 1
COMPLETED
```

## ▼ With the SL Console (SL500 libraries only)

1. **Select System Detail > Library > SNMP > Add Trap Recipients.**

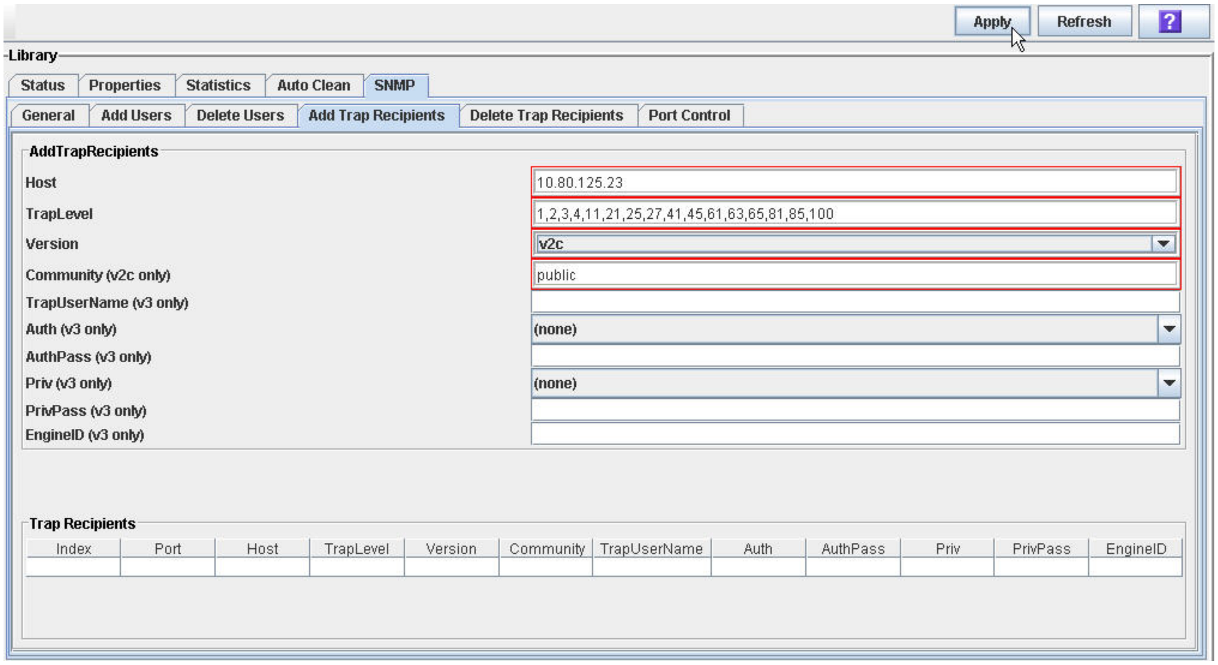


2. **To add the trap recipient, complete the Trap Recipients screen fields as follows:**

   - **Host** – Enter the IP address of the STA server.
   - **TrapLevel** – Specify the trap levels that the library should send to STA: `1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100`

     **Note –** Trap levels must be entered individually, separated by commas (`,`).

   - **Version** – Select `v2c` from the menu.
   - **Community** – This can be `public`, or another name of your choice.



AddTrapRecipients

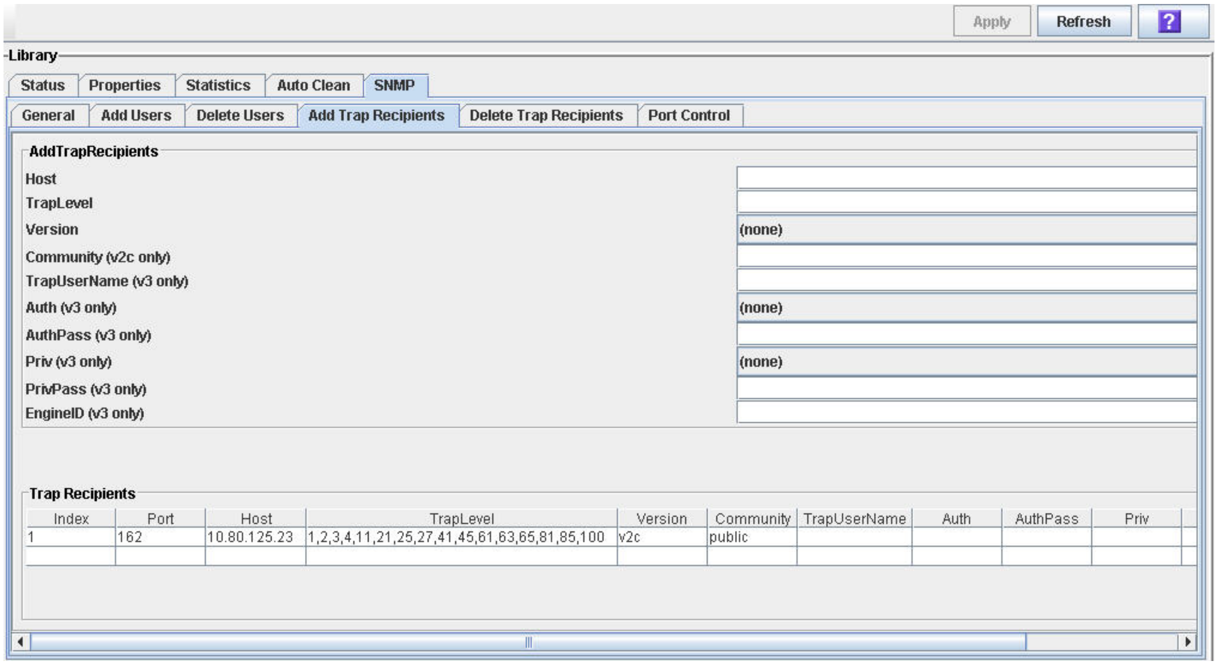
| | |
|---|---|
| Host | 10.80.125.23 |
| TrapLevel | 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100 |
| Version | v2c |
| Community (v2c only) | public |
| TrapUserName (v3 only) | |
| Auth (v3 only) | (none) |
| AuthPass (v3 only) | |
| Priv (v3 only) | (none) |
| PrivPass (v3 only) | |
| EngineID (v3 only) | |

Trap Recipients

| Index | Port | Host | TrapLevel | Version | Community | TrapUserName | Auth | AuthPass | Priv | PrivPass | EngineID |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |

3. **Click Apply.**

   The trap recipient is added and the screen is updated.



AddTrapRecipients

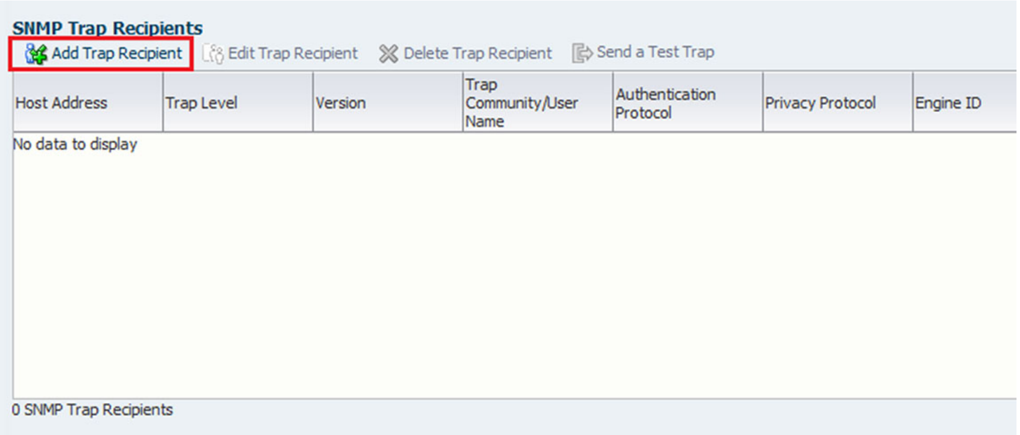
| | |
|---|---|
| Host | |
| TrapLevel | |
| Version | (none) |
| Community (v2c only) | |
| TrapUserName (v3 only) | |
| Auth (v3 only) | (none) |
| AuthPass (v3 only) | |
| Priv (v3 only) | (none) |
| PrivPass (v3 only) | |
| EngineID (v3 only) | |

Trap Recipients

| Index | Port | Host | TrapLevel | Version | Community | TrapUserName | Auth | AuthPass | Priv |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 162 | 10.80.125.23 | 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100 | v2c | public | | | | |

## ▼ With the SL150 User Interface

1. **Select Settings from the navigation bar on the left side of the interface.**
2. **Select the SNMP tab.**
3. **Under SNMP Trap Recipients, select Add Trap Recipient.**



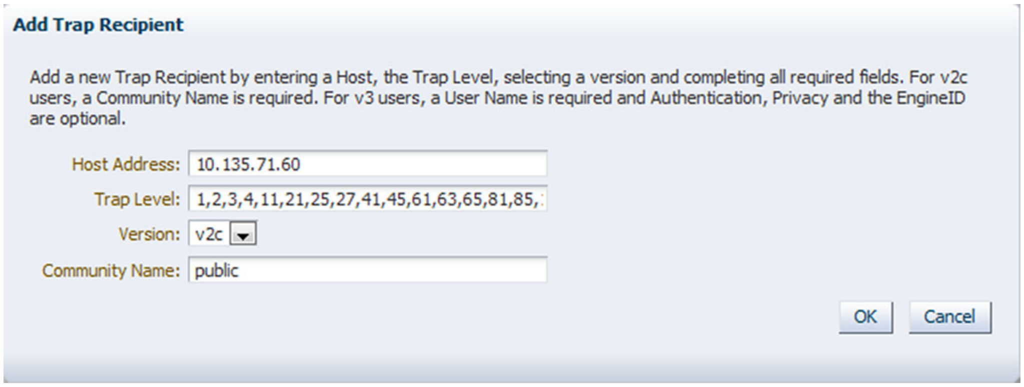
| Host Address | Trap Level | Version | Trap Community/User Name | Authentication Protocol | Privacy Protocol | Engine ID |
|---|---|---|---|---|---|---|
| No data to display | | | | | | |

0 SNMP Trap Recipients

4. **To add the trap recipient, complete the Add Trap Recipient fields as follows:**
   - **Host Address** – Enter the IP address of the STA server.
   - **Trap Level** – Specify the trap levels that the library should send to STA: `1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100`

     **Note –** Trap levels must be entered individually, separated by commas (,).
   - **Version** – Select v2c.

- **Community Name** – Can be **`public`**, or another name of your choice.



**Add Trap Recipient**

Add a new Trap Recipient by entering a Host, the Trap Level, selecting a version and completing all required fields. For v2c users, a Community Name is required. For v3 users, a User Name is required and Authentication, Privacy and the EngineID are optional.

Host Address: 10.135.71.60

Trap Level: 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,

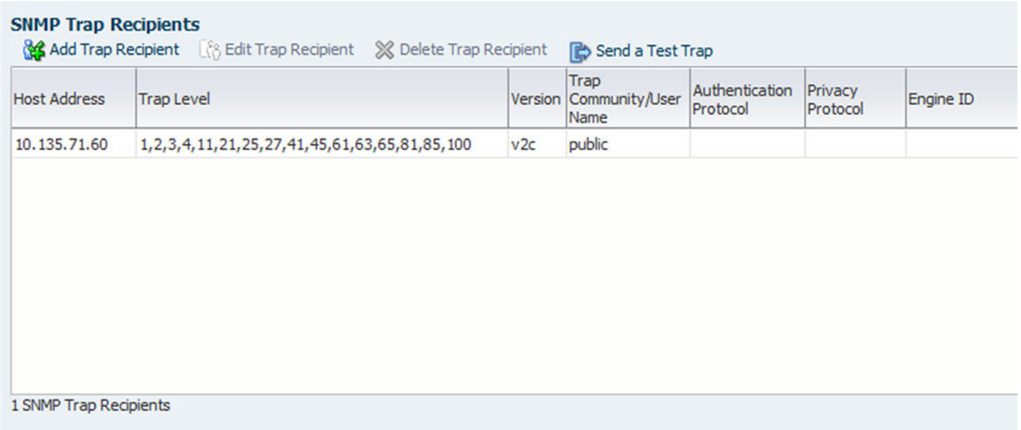
Version: v2c

Community Name: public

5. **Click OK.**

   The trap recipient is added and the screen is updated.

   > **Note –** Do not click the "Send a Test Trap" button, as test traps are not supported by STA.



**SNMP Trap Recipients**

| Host Address | Trap Level | Version | Trap Community/User Name | Authentication Protocol | Privacy Protocol | Engine ID |
|---|---|---|---|---|---|---|
| 10.135.71.60 | 1,2,3,4,11,21,25,27,41,45,61,63,65,81,85,100 | v2c | public | | | |

1 SNMP Trap Recipients

## ▼ Enable SNMP v2c Mode for STA

Use this procedure to enable SNMP v2c on the STA server. By default, the SNMP v3 protocol is enabled and v2c is disabled on STA. To allow STA to use the v2c protocol for SNMP communications, you must explicitly enable it.

1. **Establish a terminal session with the STA server and login as root.**

2. **Change to the STA configuration files directory.**

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

3. **Edit the SNMP version properties file.**

   ```
   # vi TbiSnmpVersionSupport.properties
   ```

4. **Change the value of the v2c parameter to "true".**

   ```
   V2c=true
   ```

5. **Save and exit the file.**

6. **Stop STA.**

   ```
   # STA stop
   Stopping the WebLogic staServer....
   Successfully stopped the WebLogic staServer
   Stopping the WebLogic Administration Server....
   Successfully stopped the WebLogic Administration Server
   Stopping the STA Database Server Backup Service (staservd)....
   Successfully stopped the STA Database Server Backup Service
   Stopping the STA database Server....
   Successfully stopped the STA Database Server
   #
   ```

7. **Restart STA.**

   ```
   # STA start
   Starting STA Database....
   Successfully started the STA Database
   Starting STA Database Backup Service (staservd)....
   Successfully started the STA Database Backup Service
   Starting WebLogic Administration Server....
   Successfully started the WebLogic Administration Server
   Starting WebLogic staServer....
   Successfully started the WebLogic staServer
   #
   ```

# Index

## C

certificate configuration
- establishing initial HTTPS/SSL connection 182
- oracle 181
- reconfigure WebLogic server to use a different security certificate 187
- replace Oracle certificate 194

## D

documentation, STA 11
dual TCP/IP
- additional configuration considerations 20
- configuring STA connection for 19
- library IP addresses 19
- related information 20

## E

email notification
- about 99
- add email address 105
- CAP message 101
- define SMTP server details 102
- delete email address 107
- drive message 101
- edit email address 106
- how it works 100
- library message 101
- message types 101
- PTP message 101
- test message 101
- test setup 106

## I

identity management, local users and open LDAP
- configure WebLogic local users 126
- configure WebLogic open LDAP users 131
- STA role assignment 125
- STA roles 125

identity management, RACF
- configure AT-TLS 143
- configure SSL 160
- configure WebLogic server 161
- create profiles 152
- enable mainframe support 142
- import certificate file and private key file 153
- install RACF/SSP on WebLogic console 171
- installing and configuring STA's RACF authorization facility 142
- mainframe minimum requirements 142
- set up RACF/SSP for WebLogic console 159
- test CGI routine 158

## L

library configuration
- configuration parameters 27
- create v3 trap recipient 61
- create v3 user 55
- drive ADI interface 21
- drive cleaning warning 24
- dual TCP/IP support 19
- enable ADI on library 43
- enable SNMP on library 46
- enabling ADI on drives 21
- enabling ADI on library 22
- ensure correct SL8500 complex ID 72
- ensure v2c user 49
- library complex IDs 25
- library log-in 30
- process 26
- redundant electronics support 19
- retrieve library engine ID 60
- retrieve SL150 IP address 40
- retrieve SL3000 or SL8500 IP addresses 36
- retrieve SL500 IP address 36
- set drive cleaning warning 71
- set SL150 volume label format 70
- set SL500 volume label format 68
- SNMP communication 17
- SNMP configuration for STA 17
- SNMP engine IDs 17
- unique v3 user 17
- user interfaces 14

- verify controller card version 41
- verify firmware version 34

O

Oracle Support, access to 11

P

PATH setting 110

R

redundant electronics
- additional configuration considerations 20
- configuring STA connection for 19
- library IP addresses 19
- related information 20

S

SNMP configuration
- configure client settings 80
- get latest configuration data from library 91
- library connections 84
- log in to STA 78
- process 75
- test connection to library 89
- verify communications 76
- verify library is operational 87

SNMP v2c mode
- configuration process 197
- create trap recipient 198
- enable for STA 203

STA backup
- configure backup service 114
- configure remote backup server 113
- preferences determination 112
- preferences list 111

STA resource monitor
- configure 120
- preferences determination 119
- preferences list 117

STA services
- configuration preparation 110

STA services daemon
- restart 123

T

troubleshooting
- unsuccessful SNMP connection 93
- unsuccessful trap processing 96

V

volume label formatting 23